PATENT ABSTRACTS OF JAPAN

(11)Publication number : **08-153072**
(43)Date of publication of application : **11.06.1996**

(51)Int.Cl. **G06F 15/00**
G09C 1/00
H04L 9/06
H04L 9/14

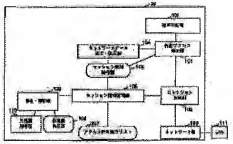
(21)Application number : **07-255169**
(22)Date of filing : **02.10.1995**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **OKAMOTO TOSHIO**
SHINPO ATSUSHI
ISHIYAMA MASAHIRO

(30)Priority
Priority number : **06261277** Priority date : **30.09.1994** Priority country : **JP**

(54) COMPUTER SYSTEM AND COMPUTER SYSTEM MANAGING METHOD

(57)Abstract:
PURPOSE: To allow a user to operate a computer without caring about difference between the managing methods of the computer that he/she actually uses and the computer of an access object by providing the system with a specified managing means and a memory means storing access permission data generated by this managing means.
CONSTITUTION: This system judges whether or not an access request from a user to each computer in another computer should be permitted, generates access permission data necessary for inspecting whether or not communication to each computer is from a user at a computer which is permitted to access each computer by one user from there, and stores it in a memory. And, access is permitted based on this. Then, a session information managing part 106 manages access from outside so that communication only from a right user outside can be executed. A session information storage part 105 stores data on a session which is permitted to access from the outside by the session information managing part 106.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－153072

(43)公開日　平成８年(1996)６月11日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｂ	9364－5Ｌ		
	Ｃ	9364－5Ｌ		
Ｇ０９Ｃ　1/00		7259－5Ｊ		Ｃ8-19
Ｈ０４Ｌ　9/06				Ｃ8-19
			Ｈ０４Ｌ　9/ 02　Ｚ	Ｃ8-19

審査請求　未請求　請求項の数19　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願平7－255169

(22)出願日　平成７年(1995)10月２日

(31)優先権主張番号　特願平6－261277

(32)優先日　平６(1994)９月30日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内

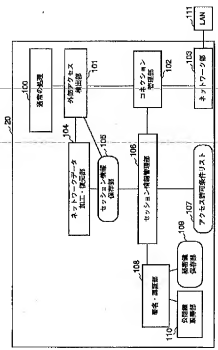
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　計算機システム及び計算機システム管理方法

(57)【要約】　（修正有）

【課題】　互いに独立した複数の計算機がネットワークを介して接続された環境において、ユーザが実際に使用する計算機とアクセス対象の計算機との管理方法の違いを意識することなく操作できること。

【解決手段】　他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断し、各計算機への通信がそこからあるユーザによる各計算機へのアクセスが許可されたある計算機におけるあるユーザからのものかどうか検査するのに必要なアクセス許可データを生成し、アクセス許可データをメモリに記憶し、かつそれに基づいて、各計算機へのアクセスが直接的になされたものか、通信手段を介して他の計算機から間接的になされたものかを検出し、後者の場合、アクセスが正当であるかどうかを判定してアクセスを許可する。



1

【特許請求の範囲】

【請求項１】　複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、

他の計算機におけるユーザから該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうか判断し、該少なくとも一つの計算機への通信がそこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、

該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、

を有することを特徴とする計算機システム。

【請求項２】　前記少なくとも一つの計算機は更に、前記複数の計算機のどの計算機におけるどのユーザが前記少なくとも一つの計算機にアクセスすることを許可されるべきかを示すアクセス許可条件を格納する格納手段を有し、該アクセス許可条件は前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて、該アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする請求項１記載の計算機システム。

【請求項３】　前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする請求項２記載の計算機システム。

【請求項４】　前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワード比較することにより判断することを特徴とする請求項２記載の計算機システム。

【請求項５】　前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする請求項２記載の計算機システム。

【請求項６】　前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする請求項１記載の計算機システム。

2

【請求項７】　前記少なくとも一つの計算機は更に、前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする請求項１記載の計算機システム。

【請求項８】　前記アクセス要求は更に、発信元ユーザ識別情報も示し、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする請求項７記載の計算機システム。

【請求項９】　前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする請求項８記載の計算機システム。

【請求項１０】　前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする請求項９記載の計算機システム。

【請求項１１】　前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする請求項１記載の計算機システム。

【請求項１２】　前記少なくとも一つの計算機が更に、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、

を有することを特徴とする請求項１記載の計算機システム。

【請求項１３】　前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、

前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする請求項１２記載の計算機システム。

【請求項１４】　前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データに対応する鍵データを記憶し、

前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする請求項１２記載の計算機システム。

【請求項１５】　前記メモリ手段は更に、前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、

前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする請求項１２記載の計算機システム。

【請求項１６】　複数の計算機群が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、

他の計算機群の計算機におけるユーザから該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうか判断し、該少なくとも一つの計算機群の計算機への通信がそこからあるユーザによる該少なくとも一つの計算機群の計算機へのアクセスが許可されたある計算機群の計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するデータ管理サーバと、

前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機へのアクセスが該少なくとも一つの計算機群において直接的になされたものか、前記通信手段を介して他の計算機群の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、前記検出手段が前記アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段と、を含むセキュリティゲートウェイと、

を有することを特徴とする計算機システム。

【請求項１７】　複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、

他の計算機におけるユーザから該計算機へのアクセス要求が許可されるべきかどうか判断し、該計算機への通信がそこからあるユーザによる該計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、

該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、

を有することを特徴とする計算機。

【請求項１８】　複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、

該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、

そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該あるお計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、

前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、

を有することを特徴とする計算機システム。

【請求項１９】　複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、

他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、

該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、

該アクセス許可データをメモリに記憶するステップと、

該メモリに記憶された該アクセス許可データに基づいて、該各計算機へのアクセスが該各計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可するステップと、

を含むことを特徴とする計算機システム管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、広域ネットワークに接続され独立管理され、管理の異なるか外部からのア

クセスが制限されている複数の計算機システムを相互に利用するユーザが、外部からのアクセスが許可され、各計算機システムやその管理の違い、例えばユーザＩＤの違いを意識しないで、自分の個人情報を利用できるユーザ識別情報管理方式を用いた計算機システム及び計算機システム管理方法に関する。

【０００２】

【従来の技術】計算機システムの小型化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへと移行している。例えば、オフィス端末やＷＳ（ワークステーション）を設置し、文書作成や表計算処理など事務処理やシミュレーションなどの技術計算に利用し、あるいはＣＡＤとして各種設計に利用し、さらには電子メールなどコミュニケーション・システムとして利用している。

【０００３】計算機システム自体の進歩に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有やオフィス外のサービスの利用、オフィス外とのコミュニケーションが可能になり、これら が広く利用されはじめた。

【０００４】例えば、特殊な処理や高速な処理を要求される科学技術計算のために外部の計算センターにスーパーコンピュータを設置し、それを共同利用している。ユーザは、リモートログイン機能を用いて、自分のＷＳをスーパーコンピュータに接続し、リモートファイルコピー機能を用いてデータを転送し、処理をスーパーコンピュータで行い、処理結果を自分のＷＳへ転送し記録媒体への格納やディスプレイへの表示を行うものである。

【０００５】また、このようなコンピュータ・ネットワーク環境を利用して、自分のＷＳを遠隔地のＷＳと結んでＷＳ会議を行ったり、電子メールを利用して意見を交換することなどが行われている。

【０００６】ＷＳ会議や電子メールの利用形態では、ユーザがコミュニケーションするのに必要な情報や処理がすべて計算機システム上で実現されている場合には非常に効果が大きい。

【０００７】さらに、グラフィック技術やファイル容量、マルチメディア技術も進歩してきている。しかし、これに対応する計算機システムやネットワークの機能は不十分である。たとえば、ＷＳ会議システムは、内容自体の伝達のためには有効利用し得るが、出席者の微妙な反応、例えば顔色をうかがったり、こちらからの迫力を伝えたりするためには、情報伝達能力が乏しい。ＴＶ会議システムのような比較的大規模なミーティングでも、現在の通信能力やＷＳの表示能力では、参加者各人が小さく表示され、解像度が低く、画面の色再現が悪かったり、動きがなめらかでないなどの問題がある。

【０００８】そこで、参加者が所定の会議場所に集まって議論するような従来方式（いわゆる対面方式）おいて、計算機システムを補助的に用いる形態も良く利用される。そして、会議場所に設置されている計算機システムは、広域ネットワークを介して各参加者が通常利用している計算機システムと接続されていることが通常である。

【０００９】しかし、会議場所に設置された計算機システムは、種々の相互に無関係な会議に連続して利用されるので普通であるので、ユーザ名やユーザＩＤ、パスワードなどのアカウントの登録は、各会議限りの一時的なものを作成することがある。この場合、参加者は、参加する会議の開催前や会議終了後に、その計算機システムを利用することはできない。さらには、参加者が会議場所の計算機システムから普段利用している計算機システムを遠隔で利用できる場合、後者の計算機システムではユーザの認証ができないので、そのままアクセスを許すには、危険が伴う。

【００１０】一方、アカウントを固定的に予め用意しておき、会議に参加するものは、だれでも会議場所に設置された計算機システム利用できるようにする方法も考えられる。この場合、異なる会議の参加者に同じアカウントを重複して割り当てることになるので、会議の前後にもアクセスできるようになるが、同一アカウントを利用する他人のファイルを見ることもできるので、情報の秘匿の点で問題がある。また、このようなアカウントのパスワードは、公開・共有する観点から覚え易いものを用いることが多いので、セキュリティの点でも不利益が生じやすい。

【００１１】また、出張先など、組織の異なるところに設置された計算機システムを利用して自分の組織の計算機を利用しようとしても、不正な外部からのアクセスを禁止し、内部の重要な情報を守るために、アクセスを禁止している場合が多い。したがって、外部から自由の自分の組織の計算機システムを利用ができないという不自由さがある。

【００１２】

【発明が解決しようとする課題】従来、同一ユーザが、ネットワークを介して接続され、異なる管理下に置かれた複数の計算機それぞれにユーザＩＤを持ち、ユーザが移動しながら各計算機を使用する場合、各計算機ごとにシステム管理、特にユーザＩＤ管理が独立して行われるので、ユーザは、ある計算機に他の計算機を介してアクセスする手続きが非常に面倒であった。また、この手続きを簡略化しようとすると、セキュリティの面で問題が生じた。

【００１３】また、管理の異なる各計算機間には、通常原則として、外部とネットワークを利用したアクセスは禁止または、非常に厳しく制限された状態になっている。よって、複数計算機を利用するユーザは、ユーザの移動ごとに、必要な計算機とアクセスできるように、ネットワークのアクセス制限を変更する必要があり、その

変更手続きと、変更作業は、非常に面倒であった。

【００１４】本発明は、上記事情を考慮してなされたものであり、互いに異なる管理下に置かれた複数の計算機がネットワークを介して接続されて環境において、ユーザが移動しながら各計算機を利用する際に、実際に使用する計算機とアクセス対象の計算機の管理方法の相違を意識することなく操作でき、かつ、相互のネットワーク経由のアクセスを可能にし、かつプログラムの秘匿性も確保できるユーザ識別情報管理方式を用いた計算機システム及び計算機システム管理方法を提供することを目的とする。

【００１５】

【課題を解決するための手段】本発明は、上記の課題を解決するために、ネットワーク上に地理的に分散し、かつ、管理が異なる計算機システム間において、ユーザがアクセスする計算機システムについて、ユーザが直接的にその計算機システムを利用しているか、ユーザが外部計算機システムからリモートでアクセスしているかを検知する。もし、リモート利用の場合、外部計算機システムつまり直接ユーザが利用している計算機システムが、その外部計算機システムでのユーザ管理情報を、リモートアクセス先の計算機システムのユーザ管理情報に反映させることで、ユーザ名やユーザＩＤの違いによる外部計算機システムからのリモートアクセスの制限をはずすと共にファイル転送やリモートログイン等の時のセキュリティホール（他人の不正利用）を防ぐ。

【００１６】また、ユーザが他のマシンを利用した場合、計算機システムごとに異なるユーザＩＤについて各計算機システムが自動的にユーザＩＤは違うがユーザ本人は同一というアクセス制御を行い、ユーザＩＤの差異を吸収するので、あるひとりのユーザが異なる計算機システムを利用しても、自分のファイルに対する適正なアクセスコントロールが自動的に設定されていたり、リモートマシンに存在する同一ユーザのファイルが自動的に転送されたりして、使い勝手が大幅に向上する。

【００１７】このために本発明は、基本的には、次のような手段を講じるものである。

・計算機へのユーザ等からのアクセス要求については、そのユーザ等がその計算機を直接利用しているかどうかを検知する。

【００１８】・外部からアクセス許可する条件は、同一ユーザに発行された各計算機におけるユーザ識別情報（例えばユーザＩＤ）及びその計算機のシステム識別情報（例えばシステムＩＤや、ネットワークアドレス）間の対応、または、各ユーザ、計算機システムごとに付与されている秘密鍵とそれに対応する公開鍵によって認証可能なユーザまたは計算機システムの署名データによって管理する。

【００１９】・外部計算機からのアクセス要求に対しては、その外部計算機のシステム識別情報やユーザ識別情報、計算機システムやユーザの署名データによる認証などからアクセス要求元を特定し、そのアクセス要求を許可するか否かをアクセス許可条件によって判断する。

【００２０】・外部の計算機からのアクセス要求を許可した場合、その許可された通信を識別する情報や、ユーザＩＤの変換に必要な情報を記憶する。

【００２１】・外部の計算機からのアクセスがあると、これが検出され、変換手順を含んだ情報に基づいてデータの変換がなされる。

【００２２】・その外部計算機上のユーザ識別情報による操作のデータが、自計算機システム上に届けられると、その外部計算機上のユーザ識別情報による操作は、自計算機システム上のユーザ識別情報からの操作とみなして扱う。

【００２３】本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、他の計算機におけるユーザから該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうかを判断し、該少なくとも一つの計算機への通信がそこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機システムを提供する。

【００２４】又、本発明は、前記少なくとも一つの計算機は更に、前記複数の計算機のどの計算機におけるどのユーザが前記少なくとも一つの計算機にアクセスすることを許可されるべきかを示すアクセス許可条件を格納する格納手段を有し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて判断することを特徴とする。

【００２５】又、本発明は、前記アクセス許可条件は前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする。

【００２６】又、本発明は、前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする。

【００２７】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワードと比較することにより判断することを特徴とする。

【００２８】又、本発明は、前記一時的パスワードは、前記少なくとも一つの計算機にて前記あるユーザに対して予め発行され、前記あるユーザは該少なくとも一つの計算機で発行された該一時的パスワードを指定して前記ある計算機から前記アクセス要求を送信することを特徴とする。

【００２９】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする。

【００３０】又、本発明は、前記有効期間は、前記少なくとも一つの計算機にて前記あるユーザにより予め指定された前記あるユーザの個人スケジュールに基づいて決定されたものであることを特徴とする。

【００３１】又、本発明は、前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする。

【００３２】又、本発明は、前記システム識別署名データは、前記発信元システム識別情報と前記発信先システム識別情報を前記他の計算機の秘密鍵を使って暗号化して求められたものであり、前記管理手段は該システム識別署名データを前記他の計算機の公開鍵を使って復号化することにより認証することを特徴とする。

【００３３】又、本発明は、前記システム識別署名データは、前記発信元システム識別情報と前記発信先システム識別情報を前記他の計算機の秘密鍵と前記少なくとも一つの計算機の公開鍵を使って暗号化して求められたものであり、前記管理手段は該システム識別署名データを前記他の計算機の公開鍵と前記少なくとも一つの計算機の秘密鍵を使って復号化することにより認証することを特徴とする。

【００３４】又、本発明は、前記少なくとも一つの計算機は更に、前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする。

【００３５】又、本発明は、前記ユーザ識別署名データは、前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする。

【００３６】又、本発明は、前記アクセス要求は更に、発信元ユーザ識別情報も示すことを特徴とする。

【００３７】又、本発明は、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする。

【００３８】又、本発明は、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする。

【００３９】又、本発明は、前記管理手段は前記少なくとも一つの計算機における前記ユーザのユーザ識別情報を更に含んだ前記アクセス許可データを生成することを特徴とする。

【００４０】又、本発明は、前記アクセス許可条件は更に前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする。

【００４１】又、本発明は、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする。

【００４２】又、本発明は、前記管理手段は更に、前記鍵データを暗号化して前記他の計算機に通知することを特徴とする。

【００４３】又、本発明は、前記少なくとも一つの計算機が更に、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、を有することを特徴とする。

【００４４】又、本発明は、前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする。

【００４５】又、本発明は、前記メモリ手段は更に、前記ある前記ユーザの前記少なくとも一つの計算機における内

部ユーザ識別情報を前記外部ユーザ識別情報と外部システム識別情報の組に対応して記憶し、前記少なくとも一つの計算機は更に、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段を有することを特徴とする。

【0046】又、本発明は、前記メモリ手段は更に、前記外部ユーザ識別情報と外部システム識別情報の組に対応する鍵データを記憶し、前記少なくとも一つの計算機は更に、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データを該通信データが示すユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記鍵データを使って加工するデータ加工手段を有することを特徴とする。

【0047】又、本発明は、前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データに対応する鍵データを記憶し、前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする。

【0048】又、本発明は、前記鍵データは前記少なくとも一つの計算機と前記ある計算機とに予め分配されており、前記ある計算機からの前記アクセスの通信データは前記鍵データから生成されたMACを含み、前記検出手段は前記アクセスが正当かどうかを前記メモリ手段に記憶された前記鍵データからMACを生成し、生成されたMACを前記アクセスの通信データに含まれるMACと比較することにより判定することを特徴とする。

【0049】又、本発明は、前記鍵データは前記少なくとも一つの計算機と前記ある計算機とに予め分配されており、前記ある計算機からの前記アクセスの通信データは前記鍵データにより暗号化されており、前記データ加工手段は前記メモリ手段に記憶された前記鍵データを使って前記アクセスの通信データを復号化することを特徴とする。

【0050】又、本発明は、前記メモリ手段は更に、前記ある計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする。

【0051】又、本発明は、前記複数の計算機は各々ユーザ識別情報に基づいて管理されており、前記アクセスが間接的なされた場合に、前記検出手段は更に前記他の計算機が前記少なくとも一つの計算機が管理されているのと同じユーザ識別情報に基づいて管理された計算機であるか、前記少なくとも一つの計算機が管理されているのと異なる他のユーザ識別情報に基づいて管理された計算機であるかを検出し、該アクセスが該他のユーザ識別情報に基づいて管理された計算機からなされたものであるとき該アクセスが正当であるかどうかを判定することを特徴とする。

【0052】更に、本発明は、複数の計算機群が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、他の計算機群の計算機におけるユーザから該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうか判断し、該少なくとも一つの計算機群の計算機へのアクセスがそこからあるユーザによる該少なくとも一つの計算機群の計算機へのアクセスが許可されたある計算機群の計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するデータ管理サーバと、前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機へのアクセスが該少なくとも一つの計算機群において直接的になされたものか、前記通信手段を介して他の計算機群の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、前記検出手段が前記アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段と、を含むセキュリティゲートウェイと、を有することを特徴とする計算機システムを提供する。

【0053】又、本発明は、前記セキュリティゲートウェイは前記検出手段と前記メモリ手段の機能を有するフィルタリングルータと、前記メモリ手段と前記データ加工手段の機能を有するデータ処理サーバとに分離されていることを特徴とする。

【0054】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、他の計算機におけるユーザから該計算機へのアクセス要求が許可されるべきかどうか判断し、該計算機へのアクセスがそこからあるユーザによる該計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成する管理手段と、該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機を提供する。

【0055】又、本発明は、前記計算機は更に、該計算機へのアクセスが該計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを前記メモリ手段

に記憶した前記アクセス許可データに基づいて判定し、正当と判定された場合、該アクセスを許可する検出手段と、を有することを特徴とする。

【００５６】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システムを提供する。

【００５７】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を示すアクセス許可条件を格納する格納手段と、該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出する検出手段と、該アクセスが間接的になされたものである場合、該アクセスが許可されるべきかどうか判断し、該アクセスが許可されるべきと判断された場合、該アクセスを許可する管理手段であって、該管理手段は前記他の計算機の発信元システム識別情報を認証し、前記他の計算機の秘密鍵で暗号化された発信元ユーザ識別情報を取得し、該発信元ユーザ識別情報を前記他の計算機の公開鍵を使って復号化することで認証し、認証された発信元ユーザ識別情報と発信元システム識別情報について前記格納手段に格納された前記アクセス許可条件を検査することにより判断するものと、前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、を有することを特徴とする計算機システムを提供する。

【００５８】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、該アクセス許可データをメモリに記憶するステップと、該メモリに記憶された該アクセス許可データに基づいて、該各計算機へのアクセスが該各計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可するステップと、を含むことを特徴とする計算機システム管理方法を提供する。

【００５９】更に、本発明は、複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムを管理する方法であって、他の計算機におけるユーザから各計算機へのアクセス要求が許可されるべきかどうか判断するステップと、該各計算機への通信がそこからあるユーザによる該各計算機へのアクセスが許可されたある計算機における該あるユーザからのものかどうか検査するのに必要なアクセス許可データを生成するステップと、該アクセス許可データをメモリに記憶するステップと、を含むことを特徴とする計算機システム管理方法を提供する。

【００６０】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について説明する。

【００６１】（第１の実施の形態）最初に、本発明の各実施の形態において基本となる第１の実施の形態を説明し、次いでいくつかのその応用の実施の形態を説明する。

【００６２】まず第１の実施の形態における全体構成を、図１に示す。この図１は、最小構成の場合で、２つの計算機システムから構成されている。

【００６３】ユーザ（利用者）が通常利用する計算機システム（ホームシステム）２と、地理的に離れた別の外部の計算機システム（遠隔システム）４がある。通常、このユーザは、ホームシステム２を利用して作業しているが、会議等の場合、出かけていって遠隔システム４を利用する。

【００６４】ホームシステム２と遠隔システム４は、各

々の計算機システムに直接接続されたＬＡＮ－Ａ８と、ＬＡＮ－Ｂ１０を介し、広域ネットワーク６によって接続されている。互いの通信は、標準的なネットワークプロトコルであるＴＣＰ／ＩＰで接続されている。ホームシステム２は、ネットワークアドレスＡで広域ネットワーク６とつながり、遠隔システム４は、ネットワークアドレスＢで広域ネットワーク６と接続されている。

【００６５】標準的なネットワークサービスは双方のシステムから利用できる。本実施の形態ではネットワークサービスのうち、ＲＦＣ９５９で規定されるリモートファイル転送プログラム（ＦＴＰ）とＲＦＣ８５４で規定されるリモートログインプログラム（ＴＥＬＮＥＴ）を使って説明する。これらのプログラムは、ユーザが起動するクライアントプログラムと、予め起動され、クライアントからのサービス要求を待つサーバプログラムから構成されている（これらのサービスの詳細は、Ｄ．Ｃｏｍｅｒ著、村井・楠木駅、「ＴＣＰ／ＩＰによるネットワーク構築　第２版」（共立出版　ｂｉｔ別冊）に詳しい。）。

【００６６】ホームシステム２と遠隔システム４は、各々所属組織が異なっているので、管理体制は独立しており、ユーザ管理（ユーザＩＤの登録、削除など）やファイル管理（ファイルごとにファイルのアクセスコントロールを設定し、また、設定されたアクセスコントロールに従ってユーザごとにファイルのアクセスを制限するなど）も計算機システムごとに独立である。

【００６７】つまり、図１の構成は、それぞれの計算機の管理が異なった、遠隔システム４とホームシステム２の２台が、広域ネットワーク６を介して接続されている場合である。

【００６８】計算機システムの種類については、ホームシステム２と遠隔システム４で計算機システムの種類は同一でも良いし、異なっていても良い。例えば、ホームシステム２と遠隔システム４ともにワークステーションシステムである場合、ホームシステム２はメインフレームシステムであり、遠隔システム４はワークステーションシステムである場合などが考えられる。

【００６９】本実施の形態の説明では、どちらの計算機システムもＵＮＩＸシステム上に構築されているとして説明する。ただし、ＴＣＰ／ＩＰをサポートしており、ＦＴＰ、ＴＥＬＮＥＴ等のサービスを提供していれば、他のＯＳ上に構築されていても同様である。

【００７０】本実施の形態では、計算機システム２，４の内部機能構成は同一であるとし、これを図２に示す。これが、以下に続く実施の形態の基本構成である。

【００７１】図２に示すように、この計算機システム２０は、通常の処理１００，外部アクセス検出部１０１，コネクション管理部１０２，ネットワーク部１０３，ネットワークデータ加工・復元部１０４，セッション情報保存部１０５，セッション情報管理部１０６，アクセス許可条件リスト１０７，署名・認証部１０８，秘密鍵保存部１０９，公開鍵取得部１１０，から構成され、ＬＡＮＩＩＩと接続されている。

【００７２】この中で、通常の処理１００，コネクション管理部１０２，ネットワーク部１０３，ＬＡＮＩＩＩは、従来の計算機、例えば、ＯＳとしてＵＮＩＸを載せたワークステーションの機能と変わらない。ユーザ管理は、通常の処理１００に含まれる。

【００７３】即ち、通常の処理１００は、ユーザが直接または間接的に利用する処理全般をいい、通常のＷＳが持つ機能を指す。具体的機能としては、ログイン処理、ファイルシステム、ユーザ管理部、電子メール、文書エディタ、ワープロ機能、プログラム開発環境、プログラム実行環境、ウィンドウシステムなど、及びネットワークを利用する処理として、リモートログイン、リモートファイル転送などを指す。

【００７４】又、コネクション管理部１０２は、ＯＳＩ７階層モデルでのトランスポート層の処理に相当し、ＴＣＰ／ＩＰにおいては、ＴＣＰやＵＤＰの処理を行う。つまり、１つの計算機システムには、ＴＣＰやＵＤＰなどのプロトコル別にポートと呼ばれる識別子があり、このポート単位で、計算機間の通信を行う。

【００７５】又、ネットワーク部１０３は、ＯＳＩ７階層モデルでのネットワーク層の処理に相当し、ＴＣＰ／ＩＰにおいては、ＩＰ処理を行う。複数のデータリンク間をルータで結ぶことによって、計算機システム間の通信が行える。

【００７６】これら以外が、本実施の形態において付加された新しい機能に該当するものである。

【００７７】即ち、セッション情報管理部１０６は、遠隔システム４からホームシステム２を利用する場合などに、外部からのアクセスを管理し、外部の正しいユーザからだけと通信できるように管理する部分である。

【００７８】又、セッション情報保存部１０５は、セッション情報管理部１０６で外部からのアクセスを許可された後述するセッションに関するデータを保存する。このデータは、外部から／外部へのアクセスであるかどうかを外部アクセス検出部１０１で検出された通信に関し、その通信が許可されたものかどうかを検査するために必要な情報である。又、このデータは、ネットワークデータ加工・復元部１０４でも用いられる。

【００７９】又、アクセス許可条件リスト１０７は、セッション情報管理部１０６で利用し、外部から自システムにアクセスしてよい利用可能な諸条件がここに保存される。

【００８０】又、署名・認証部１０８は、外部からアクセスする計算機システムのホストＩＤやユーザＩＤに関して、暗号技術を用いて認証を行い、自計算機システムのホストＩＤやユーザＩＤに関して、暗号技術を用いて署名を付ける。

【００８１】又、公開鍵取得部１１０は、認証に必要な、外部のマシンまたは、ユーザの公開鍵を検索し、取得する。

【００８２】又、秘密鍵保存部１０９は、署名に必要な、自マシンまたは、自マシン上のユーザの秘密鍵を保管する。

【００８３】又、外部アクセス検出部１０１は、外部からの通信、または、外部への通信を検出し、その通信が、許可された外部のユーザまたは、外部の計算機システムから、または、宛てのものかどうかをセッション情報保存部１０５に保存された情報を基に、検査する。

【００８４】又、ネットワークデータ加工・復元部１０４は、外部のシステムと通信する際に、通信データの安全のために、データを暗号化したり復号化したりする。また、許可された外部との通信であることを示す認証子をデータに付加したり、外部アクセス検出部１０１で検査済みのデータから認証子をはずしたりする。

【００８５】次に、図３は、複数のホームシステム６０が、同一の管理下におかれて１つのホームシステムグループ３０として構成されている場合の全体構成である。

【００８６】この場合、図３に示すように、機能ごとに複数の計算機に分割して構成してもよい。すなわち、外部ネットワークとの接続点に位置するセキュリティゲートウェイ４０、セッション情報管理を担当するセッション情報管理サーバ５０，所望の処理を行う複数のホームシステム６０からなる構成としても良い。

【００８７】各計算機システムにおける内部機能構成を図４～図６に示す。図中の点線が機能の分割によって各計算機システムにおいて不要になった機能である。

【００８８】なお、図３における遠隔システム４の内部機能構成は図１の構成における遠隔システム４の内部機能構成である図２と変わらないので説明は省略する。

【００８９】この場合図６に示すホームシステム６０は、通常の計算機システムと変わらなくなる。つまり、図３のグループ構成では、通常の計算機システムをホームシステム６０として用い、セキュリティゲートウェイ４０とセッション情報管理サーバ５０を付加することで、図３のシステム構成となる。

【００９０】図５に示すセッション情報管理サーバ５０は、ホームシステムグループ３０内に最低１台あり、ここで、外部との通信に必要なセッションの設立処理を行う。セッション設立が成功した後、必要な情報が、セッション情報保存部１０５に蓄えられる。この情報は、同時に、セキュリティゲートウェイ４０内のセッション情報保存部１０５へも送られ、蓄えられる。

【００９１】図４に示すセキュリティゲートウェイ４０は、ホームシステムグループ３０と外部とを接続する点に位置する計算機システムであって、ここを通過する通信は、外部アクセス検出部１０１で検出される。これは、このシステムに入力される通信のパケットのヘッダ情報をみて、その中の発信元、あて先のネットワークアドレスを検査することで行われる。該当パケットは、セッション情報保存部１０５のデータと比較され漏遺できるか判断される。

【００９２】外部アクセス検出部１０１の検査に合格したデータは、ネットワークデータ加工・復元部１０４で必要な処理が行われたあと通過する。

【００９３】セッション設立に必要な通信は、セキュリティゲートウェイ４０を通過し、セッション情報管理サーバ５０へ送られる。この際の外部からの通信は、セキュリティゲートウェイ４０とセッション情報管理サーバ５０間に制限されている。

【００９４】また、セキュリティゲートウェイ４０の内部機能構成においてコネクション管理部１０２のない構成もある。ネットワーク部１０３を通る通信のパケットを直接、外部アクセス検出部１０１にて検査するものである。

【００９５】なお、セキュリティゲートウェイ４０とセッション情報管理サーバ５０は、同一のマシンで構成しても良い。

【００９６】また、セキュリティゲートウェイ４０の機能をさらに分割し、図７に示すように、外部アクセス検出部１０１とそれに付随する機能を載せた計算機システム（フィルタリングルータ）７０と、図８に示すように、ネットワークデータ加工・復元部１０４、セッション情報保存部１０５とそれらに付随する機能を載せた計算機システム（ネットワークデータ処理サーバ）８０を別々の計算機システムとして実装してもよい。その場合の全体構成を図９に示す。

【００９７】もちろん、それぞれの機能に必要な、セッション情報保存部１０５は、両方の計算機システムに存在する。この構成の場合、フィルタリングルータ７０の機能を、既存のネットワークルータ装置に組み入れることが容易となる。フィルタリングルータ７０には、上記のセキュリティゲートウェイ４０と同様、コネクション管理部１０２が存在している構成もある。

【００９８】２つの構成を分けた場合、外部からの通信のデータは、フィルタリングルータ７０で検査のち、ネットワークデータ処理サーバ８０に送られる。また、ホームシステムグループ３０内のホームシステム６０から外部への通信のデータは、ルータ９０を経由してネットワークデータ処理サーバ８０へ送られ、そこからフィルタリングルータ７０経由で、外部へ送信される（図中の濃い矢印の通信経路）。

【００９９】つまり、ホームシステムグループ３０内のホームシステム６０では、外部あての通信は、一旦、ネットワークデータ処理サーバ８０に送られるように、ＩＰ層のルーティング情報が設定されている。

【０１００】さらに、外部から来た通信のデータは、安全のため、フィルタリングルータ７０と、ネットワーク

データ処理サーバ８０またはセッション情報管理サーバ５０間だけに、ＩＰ層における直接の通信が制限されている（図中の薄い矢印が直接通信可能な範囲を示している。）。

【０１０１】以下、各機能の動作を単純な構成である図２の場合について説明する。ここでの動作は、セッション設立と、セッションを用いた通信との２つの段階に大きく分かれるので、これら各段階を分けて説明する。

【０１０２】（Ｉ）セッション設立

いま、ユーザ田中さんが、ホームシステム２（ネットワークアドレス＝Ａ）上にアカウントを持っているものとする。ホームシステム２上でのユーザＩＤを１とする。このユーザ田中さんは、遠隔システム４（ネットワークアドレス＝Ｂ）にもアカウントを持っており、この遠隔システム４上のユーザＩＤを１０１とする。

【０１０３】遠隔システム４で、ユーザ田中さんが、ホームシステム２にアクセスして、ホームシステム２にログインしたり、ホームシステム２の資源（ファイルなど）をアクセスする際、実際の所望する作業に先立ち、遠隔システム４のセッション情報管理部１０６とホームシステム２のセッション情報管理部１０６との間で、ネゴシエーションを行い、アクセス許可を得る。

【０１０４】この許可の単位のことをセッションと呼ぶことにする。つまり、あるシステムのあるユーザからの通信と、別のあるシステムのあるユーザへの通信が許可された場合、その対をセッションと呼ぶ。

【０１０５】遠隔システム４では、そのユーザがそのユーザのホームシステム２にアクセスするためのセッションの設立を行い、セッションＩＤを取得する。以後の実際の所望の通信では、このセッションＩＤを用いて、ホームシステム２にアクセスすることができ、所望の作業が行える。

【０１０６】１つのセッションを設立しセッションＩＤを得るには、以下の動作を行う。ここで、クライアント側（遠隔システム４）のセッション設立時の計算機システムの機能構成を図１０に、サーバ側（ホームシステム２）の機能構成を図１１にそれぞれ示す。

【０１０７】Ｉ－１．セッション要求データの作成と送信：クライアント側（遠隔システム４）の動作

遠隔システム４のセッション情報管理部１０６は、遠隔システム４のユーザからの直接的または間接的な指示で、通常の処理１００からの指示により、ホームシステム２との間でセッションを設立する。そのため、遠隔システム４のセッション情報管理部１０６は、ホームシステム２のセッション情報管理部１０６へセッション設立のための要求データを送信する。

【０１０８】ここで、本実施の形態におけるセッション設立のために送信するデータの具体例を示す。

１．送信元ネットワークアドレス：遠隔システム４のネットワークアドレス（＝Ｂ）

２．送信元の計算機システムでのユーザＩＤ：遠隔システム４での自分のユーザＩＤ（＝１０１）

３．あて先のネットワークアドレス：ホームシステム２のネットワークアドレス（＝Ａ）

４．あて先の計算機システムでのユーザＩＤ：ホームシステム２での自分のユーザＩＤ（＝１）

５．送信元ホストの署名：遠隔システム４の署名データ

６．送信元ユーザの署名：遠隔システム４のユーザの署名データ

このセッション設立のためのデータのうち、送信元（自システムすなわち遠隔システム４）のネットワークアドレスは、ネットワーク層１０３で保持しており、ここから指示される。

【０１０９】自マシンのユーザＩＤは、セッション設立要求をしたユーザＩＤのことであり、これは、通常の処理１００の中のユーザ管理部（図示せず）で管理されている。このユーザＩＤが上記の自マシンのデータになる。

【０１１０】あて先の計算機システム（ホームシステム２）のネットワークアドレスと、そのマシンでのユーザＩＤは、このセッション設立先の計算機システム（ホームシステム２）のネットワークアドレスと、ユーザＩＤである。これらは、このセッションを設立しようとするユーザが、直接的または間接的に知らせる。

【０１１１】ここで、送信元のホストの署名は、以下のようにデータを作成して署名する。即ち、遠隔システム４のネットワークアドレスとホームシステム２のネットワークアドレスとこのデータ作成時の日時の３つのデータを遠隔システム４（自システム）のもつホスト秘密鍵で暗号化したものを送信元ホストの署名データとする。

【０１１２】又、送信元のユーザの署名は、以下のようにデータを作成して署名する。即ち、遠隔システム４のユーザＩＤとホームシステム２のユーザＩＤとこのデータ作成時の日時の３つのデータをユーザ田中さんのもつ秘密鍵で暗号化したものを送信元ユーザの署名データとする。

【０１１３】本実施の形態では、計算機システムやユーザの署名は、発信元の計算機システム（自システムつまり、遠隔システム４）内の署名・認証部１０８にて作成する。

【０１１４】署名に必要な暗号鍵については、自システム（遠隔システム４）のホスト秘密鍵やユーザの秘密鍵を秘密鍵保存部１０９から得る。ユーザの個人秘密鍵は、ユーザが移動した際に、予め、移動先の秘密鍵保存部１０９へ入力して保存しておく。

【０１１５】Ｉ－２．セッション要求データの受信とセッションの設立：サーバ側（ホームシステム）の動作

上記Ｉ－１のクライアント側の処理について遠隔システム４のセッション情報管理部１０６で作成されたセッション設立要求データは、コネクション管理部１０２、ネ

ットワーク部１０３，ＬＡＮ１１１，広域ネットワーク６を経て、ホームシステム２に届けられ、更に、ホームシステム２のＬＡＮ１１１、ネットワーク部１０２、コネクション管理部１０２を経てホームシステム２のセッション情報管理部１０６へ届く。

【０１１６】ここでは、セッション設立要求した、送信元のホストとユーザの認証を行い、今後の実際の所望の作業の処理を実行して良いか判断する。具体的には以下の処理ｘ－１～ｘ－７を行う。

処理ｘ－１　送られてきたデータ中の送信元ホストの送信元ユーザの認証を行う。

処理ｘ－２　図示しない時計などにより、送られたデータが、有効期間内かチェックする。

処理ｘ－３　上記２つの条件に合致したら、図１２に示すようなアクセス許可条件リスト１０７の内容と比較し、要求元のホストやユーザが今後、自システムにアクセスしてよいか判断する。

処理ｘ－４　アクセスが許可されると、新たにセッションを１つ生成し、セッションＩＤが振られる。

処理ｘ－５　そのセッションに関するセッション情報をセッション情報保存部１０５に蓄える。その中には、新たに生成され、以後の実際の所望の作業のための通信で必要になるセッション鍵（そのセッションでのみ有効な一時的暗号鍵）が含まれる。

【０１１７】セッション情報保存部１０５に蓄えるデータの一例を図１３に示す。この図１３に示すように、このセッション情報中には、以下に示す内容が含まれる。

１．自計算機システム（ホームシステム２）でのユーザＩＤ

２．対応する外部計算機システム（遠隔システム４）でのネットワークアドレス

３．対応する外部計算機システム（遠隔システム４）でのユーザＩＤ

４．そのセッションのセッションＩＤ

５．そのセッションに有効なセッション鍵

６．有効期間

【０１１８】処理ｘ－６　セッション設立に成功すると、セッション要求元である計算機システム（遠隔システム４）にアクセスを許可する旨の回答データを作成して送付する。具体的には、この回答データは以下の内容を含む。

１．送信元ネットワークアドレス：ホームシステム２のネットワークアドレス（＝Ａ）

２．送信元の計算機システムでのユーザＩＤ：ホームシステム２での自分のユーザＩＤ（＝１）

３．あて先のネットワークアドレス：遠隔システム４のネットワークアドレス（＝Ｂ）

４．あて先の計算機システムでのユーザＩＤ：遠隔システム４での自分のユーザＩＤ（＝１０１）

５．送信元ホストの署名：ホームシステム２の署名データ

６．送信元ユーザの署名：ホームシステム２のユーザの署名データ

７．セッションＩＤ：そのセッションを識別するＩＤ

８．セッション鍵：そのセッションで有効な一時的暗号鍵

９．有効期間：そのセッションの有効な期間

【０１１９】ここで、送信元を特定するため（偽のホームシステムでないことを検査するため）に、送信元のホスト名とユーザ名の署名を付ける。署名の付け方は、上述したセッション設立要求時の署名作成の処理と同様である。

【０１２０】同時に返送する、セッション鍵も別のホストで解読されないように、以下の処理を行って送られる。即ち、セッション鍵をあて先のホスト（遠隔システム４）の公開鍵と送信元のホスト（ホームシステム２）の秘密鍵で暗号化してから送付する。

【０１２１】処理ｘ－７　アクセス許可条件に適合せず、セッション設立に失敗すると、その旨のデータを送信元である計算機システム（遠隔システム４）に返す。

【０１２２】ここで、上記の処理ｘ－１の認証処理を更に詳しく説明する。送られてきたデータのうち、送信元ホスト（遠隔システム４）の認証は、ホスト認証のための署名データを用い、このデータを遠隔システム４の公開鍵を用いて復号化する。

【０１２３】復号化された平文中に書かれている送信元ホストアドレスとあて先ホストアドレスがそれぞれ、遠隔システム４とホームシステム２のアドレスに一致し、かつ、日時データが本認証処理を行っている時間と、予め定めてある期間以内であれば、認証成功と判断する。

【０１２４】送信元ホストのユーザの認証は、送られたデータ中のユーザ認証のためのデータを用いる。あて先ユーザＩＤのデータから、自システム（ホームシステム２）のユーザＩＤに該当するユーザ名を通常の処理１００の中に含まれるユーザ管理部（図示せず）から求め、そのユーザ名に対応する公開鍵を公開鍵取得部１１０から得て、これを用い復号化する。

【０１２５】復号化された平文中に書かれている送信元（遠隔システム４）のユーザＩＤとあて先（ホームシステム２）のユーザＩＤが、要求データ中の各々に一致し、かつ、日時データが、本認証処理を行っている時間と、予め定めてある期間以内であれば、認証成功と判断する。

【０１２６】この認証処理で使う遠隔システム４の公開鍵とユーザの公開鍵は、公開鍵取得部１１０より得る。ここに該当する公開鍵が保存されていなければ、ここからネットワーク部１０３を経て外部の公開鍵サーバ（図示せず）より入手する。

【０１２７】Ｉ－３．Ｎセッション要求の回答データの受信：クライアント側（遠隔システム４）の動作

遠隔システム４では、ホームシステム２からセッション設立の要求に対する回答データを受けとると、遠隔システム４のセッション情報管理部１０６が、受け取ったデータからセッション情報保存部１０５にデータを保存する。

【０１２８】ここでセッション情報保存部１０５に保存されるデータは、具体的には、以下のデータを含む。

１．自計算機システム（遠隔システム４）でのユーザＩＤ

２．対応する外部計算機システム（ホームシステム２）のネットワークアドレス

３．対応する外部計算機システム（ホームシステム２）でのユーザＩＤ

４．そのセッションのセッションＩＤ

５．そのセッションに有効なセッション鍵

６．有効期間

【０１２９】受信したデータ中のホスト署名とユーザ署名を検査し、セッション設立要求先のホストからの正当な回答であることを確認する。署名の認証方法は、上記処理ｘ－１の場合と同様である。

【０１３０】また、セッション鍵は暗号化されているので、自ホストの秘密鍵と相手ホストの公開鍵を用いて、上記処理ｘ－１と同様の方法で復号して元通りのセッション鍵を得る。

【０１３１】（II）セッションを用いた通信

セッション設立処理が終了すると、所望の処理が開始できる。ここでは各計算機システムが図１４の機能構成となり、クライアント側の処理と、サーバ側の処理が以下のように行われる。

II－１．クライアント側の動作

II－１－１：送信

許可された外部の計算機システム（遠隔システム４）が、ホームシステム２にデータを送信する。送信データは、通常の処理１００の部分で作成され、特別な処理を行わずに送信され、外部アクセス検出部１０１へ送られる。

【０１３２】外部アクセス検出部１０１ではデータのあて先を検出する。コネクション管理部１０２がＴＣＰの処理を行っているとすると、各通信コネクションごとに通信相手のホストのネットワークアドレスやＴＣＰのポート番号などを管理しているので、ここから必要な情報が得られる。外部アクセス検出部１０１は、この情報をセッション情報保存部１０５のデータと比較してここを通過するデータが外部あてのデータかどうか判断する。

【０１３３】外部あてのデータであると、これがネットワークデータ加工・復元部１０４に送られ、データの加工が行われる。内部あてであると、そのまま素通りし、通常の通信どおり、コネクション管理部１０２、ネットワーク部１０３を通り、ＬＡＮ１１１を経て、あて先へ送信される。

【０１３４】ネットワークデータ加工・復元部１０４に送られたデータは、必要な処理が施される。一例としては、このデータのあて先（ホームシステム２）に対して、許可された外部ホストからのデータであることを示すためにＭＡＣ（Message Authentication Code ）をセッションＩＤと共に付加する。このＭＡＣを得るには、あて先ごとに保存されているセッション情報保存部１０５のセッション鍵を用いる。これを用いて、送信データのハッシュ値を計算し、ＭＡＣ値とする。ハッシュ値の計算方法は、ＲＦＣ１３２１で規定されるＭＤ５による。

【０１３５】さらに、送信するデータの重要度や途中の通信経路によっては、データの盗聴防止のため、暗号化処理が必要になる。その場合には、ＭＡＣを生成する時に利用した同じセッション鍵を用いてたとえばＤＥＳ方式でデータ自身を暗号化する。

【０１３６】いずれの場合も、送信するデータに加工したので、それに伴って送信データのパケットフォーマットの変更も必要に応じて行う。

【０１３７】ネットワークデータ加工・復元部１０４で加工された外部あてのデータは、再び外部アクセス検出部１０１に戻り、コネクション部１０２、ネットワーク部１０３、ＬＡＮ１１１を経て、外部ネットワーク６経由であて先であるホームシステム２へ送られる。

【０１３８】なお、上記の処理では、外部あてのデータを外部アクセス検出部１０１においてセッション情報保存部１０５のデータと比較して検出していたが、外部あてのデータの検出は、簡略して次のようにして行っても良い。

【０１３９】つまりホームシステムグループにて利用している範囲のネットワークアドレスを予め、外部アクセス検出部１０１内に保存し、それを使って、通信のデータのあて先を外部あてのものかどうか判断してもよい。

【０１４０】外部あてと判断されたデータは、ネットワークデータ加工・復元部１０４に送られ、ここで、セッション情報保存部１０５のデータと比較し、真に外部へアクセス許可された通信のデータか判断し、ＭＡＣの付加等の処理を行う。

【０１４１】II－１－２：受信

外部ホスト（ホームシステム２）からの受信データは、ＬＡＮ１１１、ネットワーク部１０３、コネクション管理部１０２と通って、外部アクセス検出部１０１に届く。ここで、外部からの通信かどうか検出され、外部からアクセス可能な通信か検査される。この判断に必要な情報は、セッション情報保存部１０５から得られる。

【０１４２】内部からのデータであると、そのまま外部アクセス検出部１０１を素通りし、通常の処理１００へ渡される。

【０１４３】外部からのアクセスの場合、さらに、ネットワークデータ加工・復元部１０４に送られ、必要に応

じてデータの復元がなされる。復元に必要な情報は、セッション情報保存部１０５から得られる。そして、復元後、外部アクセス検出部１０１を経て、自システム内の通常の処理１００に引き渡される。

【０１４４】詳細に説明すると、コネクション管理部１０２が通ったデータは、外部アクセス検出部１０１で、データの発信元を検査される。コネクション管理部１０２がＴＣＰの処理を行っているとすると、各通信コネクションごとに通信相手のホストのネットワークアドレスやＴＣＰのポート番号などを管理しているので、ここから必要な情報が得られる。つまり、ＩＰパケットのヘッダ情報の中からあて先と送信元のＩＰアドレス、ＴＣＰのヘッダ情報からあて先と送信元のポート番号が得られる。この情報を、セッション情報保存部１０５のデータと比較し、外部からのアクセスかどうか判断する。

【０１４５】また、データ中にＭＡＣが入っている時は、このＭＡＣを用いて外部から可能な通信か検査できる。ＭＡＣを生成した処理と同様に、このデータ中からセッションＩＤを得、それに対応したセッション鍵をセッション情報保存部１０５から得、そのセッション鍵を利用して、ＭＡＣを生成したのと同じ手順で計算する。計算結果がデータ中に書かれているＭＡＣの値と一致するか検査し、正しいアクセスか判断する。

【０１４６】ＩＩ－２：サーバ側の処理

サーバ側の処理も上述したクライアント側と同様である。ただし、ネットワークデータ加工・復元部１０４の処理において、さらに、外部から受け取ったデータのセッションＩＤを用いて、データ中に記述されているユーザＩＤを遠隔システム４のユーザＩＤからホームシステム２のユーザＩＤに変換したり、外部へ送るデータ中のホームシステム２のユーザＩＤを遠隔システム４のユーザＩＤに変換したりする、ユーザＩＤ変換処理を合わせて行うこともできる。

【０１４７】その結果、通常の処理１００において、ホームシステム２の該当ユーザＩＤのアクセス権限で、リモートファイル転送によるファイルシステムに対するコピーなどのファイル操作やリモートログインなどのアクセスが可能になる。

【０１４８】（第２の実施の形態）次に、本発明の第２の実施の形態について説明する。この第２の実施の形態の全体構成は、上述した図１と同様である。

【０１４９】ユーザ（利用者）が通常利用する計算機システムと（ホームシステム）２と、地理的に離れた別の外部の計算機システム（遠隔システム）４がある。通常、このユーザは、ホームシステム２を利用して作業しているが、会議等の場合、出かけていって遠隔システム４を利用する。

【０１５０】ホームシステム２と遠隔システム４は、各々の計算機システムに直接接続されたＬＡＮ－Ａ８と、ＬＡＮ－Ｂ１０を広域ネットワーク６によって接続されている。互いの通信は、標準的なネットワークプロトコルであるＴＣＰ／ＩＰで接続されている。ホームシステム２は、ネットワークアドレスＡで広域ネットワーク６とつながり、遠隔システム４は、ネットワークアドレスＢで広域ネットワーク６と接続されている。

【０１５１】標準的なネットワークサービスは双方のシステムから利用できる。本実施の形態ではネットワークサービスのうち、リモートファイル転送プログラム（ＦＴＰ）とリモートログインプログラム（ＴＥＬＮＥＴ）を使って説明する。これらのプログラムは、ユーザが起動するクライアントプログラムと、予め起動され、クライアントからのサービス要求を待つサーバプログラムから構成されている。

【０１５２】ホームシステム２と遠隔システム４は、各々所属組織が異なっているので、管理体制は独立しており、ユーザ管理（ユーザＩＤの登録、削除など）やファイル管理（ファイルごとにファイルのアクセスコントロールを設定し、また、設定されたアクセスコントロールに従ってユーザごとにファイルのアクセスを制限するなど）も計算機システムごとに独立である。

【０１５３】計算機システムの種類については、ホームシステム２と遠隔システム４で計算機システムの種類は同一でも良いし、異なっていても良い。例えば、ホームシステム２と遠隔システム４ともにワークステーションシステムである場合、ホームシステム２はメインフレームシステムであり、遠隔システム４はワークステーションシステムである場合などが考えられる。

【０１５４】本実施の形態の説明では、どちらの計算機システムもＵＮＩＸシステム上に構築されているとして説明する。ただし、ＴＣＰ／ＩＰをサポートしており、ＦＴＰ、ＴＥＬＮＥＴ等のサービスを提供していれば、他のＯＳ上に構築されても同様である。

【０１５５】本実施の形態では、計算機システム２，４の内部機能構成は同一であるとし、これを図１５に示す。図１５に示すように、この計算機システム１５０は、入出力部２０１，ローカルログイン２０２，外部アクセス検出部１０１，アクセス許可条件リスト１０７，ユーザ管理部２０３，個人スケジュール管理部１５１，リモートログイン２０４，リモートファイル転送２０６，ファイルシステム２０５，ユーザＩＤ共通化部１０６Ａ，ユーザＩＤ対応管理表１０５Ａ，コネクション管理部１０２，ネットワーク部１０３，一時的パスワード入力１５２，一時的パスワード生成１５３から構成される。

【０１５６】上記第１の実施の形態との比較では、通常の処理１００と対応するものは、入出力部２０１，ローカルログイン２０２，リモートログイン２０４，ユーザ管理部２０３，リモートファイル転送２０６，ファイルシステム２０５である。図２のセッション情報管理部１０６には、ユーザＩＤ共通化部１０６Ａが対応し、図２

のセッション情報保存部１０５とは、ユーザＩＤ対応管理表１０５Ａが対応する。また、図２のネットワークデータ加工・復元部１０４に相当するところは存在せず、図２の署名・認証部１０８，公開鍵取得部１１０，秘密鍵保存部１０９に対応するものもなく、代わりに、個人スケジュール管理部１５１と一時的パスワード入力１５２と一時的パスワード生成１５３が新たに付加されている。

【０１５７】ここで入出力部２０１は、ユーザが計算機システム２，４を直接使用するための入力装置及び出力装置から構成される。入力装置としては、キーボード、マウス、さらには、シリアル回線等を利用することができる。出力装置としては、ディスプレイ、プリンタ、さらには、シリアル回線などを利用することができる。入出力部２０１は、ローカルログイン２０２を介して、内部の構成部分に接続される。

【０１５８】次に、この第２の実施の形態における動作を説明する。いま、あるユーザ田中さんが、ホームシステム２上にアカウントをもっているものとする。そのホームシステム２上でのユーザＩＤを１とする。このユーザ田中さんは、遠隔システム４にもアカウントを持っており、その遠隔システム４上のユーザＩＤを１０１とする。

【０１５９】ホームシステム２上には、個人スケジュール管理部１５１が稼働していて、個人ごとのスケジュールを管理している。ここで用いるスケジュール管理表の例を図１６に示す。個人スケジュール管理部１５１は図１６のように、ユーザごとにスケジュールの内容を書いた表をもっている。例では、田中さん（ユーザＩＤ＝１）は、「本日午後遠隔システムへ行って、作業をする」ことになっている。

【０１６０】外出する際に、田中さんは、ホームシステム内の一時的パスワード生成１５３に、出先の計算機システム（遠隔システム４）から当該ホームシステム２を使用するために必要な一時的パスワードを発行してもらう。

【０１６１】一時的パスワード生成１５３は、以下に示す処理ａ－１～処理ａ－６を行って、一時的パスワードを発行する。

処理ａ－１　要求ユーザのユーザＩＤを得る。

処理ａ－２　そのユーザＩＤのスケジュールデータを個人スケジュール管理部１５１から得る。

処理ａ－３　外出先のネットワークアドレスと外出期間をスケジュール管理表から得る。

処理ａ－４　その外出先を識別するための一時的なパスワード（第１の実施の形態におけるセッションＩＤに相当）の生成と、有効期間の計算をする。

処理ａ－５　アクセス許可条件リスト１０７に、図１７のように、「ユーザＩＤ」、「外出先ネットワークアドレス」、「一時的パスワード」、「有効期間」、「その他の情報（ファイル読みだしのみ許可などその他の許可条件など）」を登録する。

処理ａ－６　要求ユーザに一時的パスワードを返す。

【０１６２】次に、ユーザ田中さんの外出先の遠隔システム４での動作を説明する。ユーザ田中さんは、外出先に行き、そこにある遠隔システム４を使用して作業を行う。ユーザ田中さんは、遠隔システム４上のユーザアカウントを作成し、または以前作成して使っていたユーザＩＤを利用して、所望の作業を行う。ユーザ田中さんのユーザＩＤは１０１とする。ユーザ田中さんが、遠隔システム４からホームシステム２にアクセスする際には、予め、遠隔システム４で作業するユーザ田中さんからの起動により、遠隔システム４のユーザＩＤ共通化部１０６Ａで、図１８に示すような、上記セッション設立に相当するユーザＩＤ共通化のためのユーザＩＤ共通化要求のデータを作成し、ホームシステム２のユーザＩＤ共通化部１０６Ａとコネクションを張り、ユーザのＩＤの共通化作業を行う。

【０１６３】ここで、本実施の形態におけるユーザＩＤ共通化の要求のためのデータの具体例を示す。

１．送信元ネットワークアドレス：遠隔システム４のネットワークアドレス（＝Ｂ）

２．送信元の計算機システムでのユーザＩＤ：遠隔システム４での自分のユーザＩＤ（＝１０１）

３．あて先のネットワークアドレス：ホームシステム２のネットワークアドレス（＝Ａ）

４．あて先の計算機システムでのユーザＩＤ：ホームシステム２での自分のユーザＩＤ（＝１）

５．あて先の一時的パスワード生成１５３から得た一時的パスワード

【０１６４】上記のユーザＩＤ共通化の要求のためのデータのうち、送信元（自システム即ち遠隔システム４）のネットワークアドレスとユーザＩＤは、自動的に作成される。つまり、自ネットワークアドレスは、ネットワーク部１０３で保持しており、ユーザＩＤは、ユーザ管理部２０３で保持している。

【０１６５】あて先の計算機システム（ホームシステム２）の一時的パスワード生成１５３から発行された一時的パスワードは、ユーザから入力させて一時的パスワード入力１５２に情報を得る。

【０１６６】次に、遠隔システム４からユーザＩＤ共通化の要求のためのデータが送られてきたホームシステム２側では、ユーザＩＤ共通化部１０６Ａにて、以下の処理ｂ－１～処理ｂ－５の手順でユーザ共通化の判断と登録を行う。処理ｂ－１　送られてきたデータが図７のアクセス許可条件リスト１０７の内容と合致するか検査する。処理ｂ－２　図示しない時計などにより、現在が有効期間内かチェックする。処理ｂ－３　そのほかの条件があれば、それに適合するか検査する。処理ｂ－４　上記３の条件に合致したら、図１９に示すようにユーザＩ

Ｄ対応管理表１０５Ａにアクセス許可データを登録し、送信元である計算機システム（遠隔システム４）にアクセスを許可する旨を通知する。

【０１６７】なお、アクセス許可データとしての登録内容を以下に示す。

１．自計算機システム（ホームシステム２）でのユーザＩＤ

２．対応する外部計算機システム（遠隔システム４）のネットワークアドレス

３．対応する外部計算機システム（遠隔システム４）でのユーザＩＤ

４．有効期間

５．その他の情報

処理ｂ－５　上記３つの条件に合致しなければ、その旨のデータを発信元である計算機システム（遠隔システム４）に返す。

【０１６８】以後、許可された外部の計算機システム（遠隔システム４）のユーザＩＤからの所望の処理に伴う指示に従い、上記のユーザＩＤ対応管理表１０５Ａに従った自計算機システム（ホームシステム２）に該当するユーザＩＤのアクセス権限でアクセスされる。例えば、リモートファイル転送によるファイルシステムに対するコピーなどのファイル操作やリモートログインなどのアクセスが可能になる。

【０１６９】たとえば、ユーザ田中さんは、遠隔システム４を利用しており、ホームシステム２のファイルをコピーしたいとき、リモートファイル転送プログラムを利用する。この時の手順は、以下のような処理ｃ－１～処理ｃ－１２となる。なお、この手順にて交換される情報の流れを、図２０に示す。

【０１７０】処理ｃ－１　ユーザ田中さんは、遠隔システム４のリモートファイル転送２０６（クライアント側）をユーザＩＤ＝１０１の権限として起動させる。

【０１７１】処理ｃ－２　そのプログラムは、外部アクセス検出部１０１、コネクション管理部１０２、ネットワーク部１０３，ＬＡＮ１１１を経て相手計算機システム（ホームシステム２）と通信路を設定し（ＩＰデータグラム通信が可能になる）、ＴＣＰのコネクション設定を要求する。本実施の形態では、クライアント側の外部アクセス検出部１０１は、素通りで動作しない。

【０１７２】処理ｃ－３　相手計算機システム（ホームシステム２）のネットワーク部１０３を通り、コネクション管理部１０２へ要求がくる。

【０１７３】処理ｃ－４　相手計算機システム（ホームシステム２）のコネクション管理部１０２では、発信元計算機システム（遠隔システム４）とのＴＣＰのコネクションを張り、外部アクセス検出部１０１を通り、リモートファイル転送２０６（サーバ側）を起動しようとする。

【０１７４】処理ｃ－５　ホームシステム２の外部アクセス検出部１０１は、上記のコネクション要求を検出し、接続の可否の判断処理を開始する。つまり、コネクション管理部１０２へ、発信元計算機システム（遠隔システム４）のネットワークアドレスとユーザＩＤを要求する。

【０１７５】処理ｃ－６　上記コネクション管理部１０２では、ネットワークのコネクションを張る段階で発信元計算機システム（遠隔システム４）のネットワークアドレスやコネクション識別子（ポート番号）が得られている。これは、ＴＣＰのプロトコルの仕様に基づくものである。

【０１７６】処理ｃ－７　更に、発信元計算機システム（遠隔システム４）のコネクション管理部１０２に付随する図示しないユーザ・コネクション対応管理部に問い合わせることにより、このコネクションを張った発信元計算機システム（遠隔システム４）のユーザＩＤなどの情報が得られる。ユーザＩＤとコネクションの対応は、identificationプロトコル（ＲＦＣ１４１３などで規定）に従って決められているものである。

【０１７７】処理ｃ－８　受信側計算機システム（ホームシステム２）のコネクション管理部１０２は、上記２つのデータ（発信元ネットワークアドレスとユーザＩＤ）を要求元計算機システム（遠隔システム４）の外部アクセス検出部１０１に伝える。

【０１７８】処理ｃ－９　受信側計算機システム（ホームシステム２）の外部アクセス検出部１０１は、これらのデータをセッション情報保存部１０５のデータと比較して合っているか検査し、このコネクションをリモートファイル転送２０６（サーバ側）につなげるかの判断をする。

【０１７９】処理ｃ－１０　検査に合格すると、外部アクセス検出部１０１では、外部の計算機システム（遠隔システム４）との間のコネクションをリモートファイル転送２０６（サーバ側）につなぎ、実際のファイル転送の処理を開始できる状態にする。

【０１８０】処理ｃ－１１　検査に合格しないと発信元計算機システム（遠隔システム４）に不許可の返事を返し、コネクションの切断をコネクション管理部１０２へ指示する。

【０１８１】処理ｃ－１２　合格した場合、リモートファイル転送が遠隔システム４のユーザに対し利用可能になり、遠隔システム４側のリモートファイル転送２０６（クライアント側）は、通常の処理を開始する。つまり、ログイン処理を行い、遠隔システム４のユーザに、ホームシステム２のユーザＩＤとパスワードを要求し、ログインに成功すると、実際のファイル転送の処理を行う。

【０１８２】リモートログイン処理の場合も同様に、外部の計算機システム（遠隔システム４）のネットワークアドレスとユーザＩＤでアクセス許可の判定を行ってか

ら、実際の処理をはじめることができる。

【0183】以上説明したように、本実施の形態によれば、管理や計算機システムの構成の異なる複数の計算機システムをネットワークを介して接続した分散環境において、各計算機システムでユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全にファイルなどの個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【0184】すなわち、本実施の形態では、予め、ユーザＩＤごとのスケジュール管理表に移動先に計算機システムを特定する情報、例えばネットワークアドレスを記入しておき移動し、移動先の計算機システムからリモートアクセスするので、そこに記入された移動先からしかリモートアクセスできず、セキュリティが強化される。さらに移動先に予めわかっているので、移動先で必要になるファイルの先送りが可能になる。また、電子メールの到着を移動先に回送することも可能になり、移動先でのユーザの利便は著しく向上する。

【0185】又、移動先のユーザＩＤと移動元のユーザＩＤが同一ユーザであるかどうかの判断は、計算機システムにログインするためのパスワードでなく、その時の移動に関する一時的なパスワードであるので、パスワードの盗聴によるパスワードの漏洩の危険が著しく低下される。

【0186】本実施の形態では、計算機システムやユーザの識別のために、ネットワークアドレスやユーザＩＤＥを利用したが、別の識別名、例えばネットワークアドレスの代わりにシステムＩＤ、ホスト名、ドメイン名などを利用し、ユーザＩＤの代わりにユーザ名、電子メールアドレスのようなユーザ名とドメイン名を組にしたものなどを利用しても良い。

【0187】尚、本実施の形態では、外出先の遠隔システム４とホームシステム２間で、ユーザＩＤ共通化処理を行う際、要求データの中に、一時的パスワードをそのまま入れて、ホームシステム２に送っていたが、上記第１の実施の形態のように、この一時的パスワードを暗号鍵として用い、遠隔システム４からパスワードそのものを送るのではなく、ユーザ名や、遠隔ホスト名、日時データなどをその鍵で暗号化して送り、受け手のホームシステム２では、そのユーザに対応する一時的パスワードを暗号鍵として復号化して検査することも可能である。

【0188】（第３の実施の形態）次に、本発明の第３の実施の形態について説明する。この第３の実施の形態の全体構成は、上述した図１と同様である。

【0189】本実施の形態では、計算機システム２，４の内部機能構成は同一であるとし、これを図２１に示す。図２１に示すように、この計算機システム２１０は、入出力部２０１，ローカルログイン２０２，外部アクセス検出部１０１，ユーザ管理部２０３，リモートログイン２０４，リモートファイル転送２０６，ファイルシステム２０５，ユーザＩＤ共通化部１０６Ａ、コネクション管理部１０２，ネットワーク部１０３，個人秘密鍵入力部２１３，署名・認証部１０８，公開鍵取得部１１０，秘密鍵保存部１０９，計算機システム秘密鍵保存部２１２，ユーザＩＤ対応管理表１０５Ａから構成される。

【0190】上記第１の実施の形態との比較では、通常の処理１００と対応するものは、入出力部２０１，ローカルログイン２０２，リモートログイン２０４，ユーザ管理部２０３，リモートファイル転送２０６，ファイルシステム２０５である。図２のセッション情報管理部１０６には、ユーザＩＤ共通化部１０６Ａが対応し、図２のセッション情報保存部１０５とは、ユーザＩＤ対応管理表１０５Ａが対応する。又、図２のアクセス許可リスト１０７とネットワークデータ加工・復元部１０４に相当するところは存在せず、秘密鍵保存部１０９に、個人秘密鍵入力部２１３と計算機システム秘密鍵保存部２１２が付加されている。

【0191】次に、この第３の実施の形態における動作を説明する。

【0192】両システム２，４をつなぐ、ネットワークプロトコルは、上記第１，第２の実施の形態と同様ＴＣＰ／ＩＰとする。従って、ネットワーク部１０３はＩＰ処理を行い、コネクション管理部１０２はＴＣＰの処理を行う。また、ＴＥＬＮＥＴ、ＦＴＰ等のサービスも実行できるものとする。

【0193】いま、ユーザ田中さんが、ホームシステム２上にアカウントを持っているものとする。そのホームシステム２上でのユーザＩＤを１とする。このユーザ田中さんは、遠隔システム４にもアカウントを持っており、その遠隔システム４上のユーザＩＤを１０１とする。

【0194】まず、本実施の形態における認証方式について説明する。認証は、個人と計算機システムの両方で可能であり、公開鍵暗号方式で認証を行うことができる。つまり、ユーザ個人や計算機システムは、自己固有の秘密鍵をもっている。この秘密鍵は、非公開で、計算機システムやユーザ自己で安全に管理する。計算機システムの秘密鍵は、計算機システム秘密鍵保存部２１２に安全に保存されている。これは、ＯＳのカーネル内など、そのシステムで安全な部分に保存されている。ユーザ個人の秘密鍵は、他人には知られない形かつユーザ本人が必要な時に移動先でも使えるように、ＩＣカードや、磁気カードなどに記憶させておくのが好ましい。

【0195】この秘密鍵とペアになる公開鍵は、公開鍵サーバ等に登録し、各計算機システム内の公開鍵取得部１１０で自由に検索して取得できる。

【0196】従って、各ユーザは、ユーザ固有の秘密鍵を安全な形で持って外部に出向き、外部の利用先からそ

の個人の秘密鍵を用いてアクセスする。

【０１９７】よって、ユーザ田中さんは、田中さん個人しか知らない秘密鍵をもっている。これを、本実施の形態では、公開鍵暗号方式で実現する。

【０１９８】次に、ユーザ田中さんの外出先の遠隔システム４での動作を説明する。ユーザ田中さんは、外出先にいき、そこにある遠隔システム４を使用して作業を行う。ユーザ田中さんは、遠隔システム４上のユーザアカウントを作成し、または、以前作成して使っていたユーザＩＤを利用して、所望の作業を行う。ユーザ田中さんのユーザＩＤはＩ０１とする。ユーザ田中さんが、遠隔システム４からホームシステム２にアクセスする際には、予め、遠隔システム４で作業するユーザ田中さんからの起動により、遠隔システム４のユーザＩＤ共通化部１０６Ａで、図２２に示すような、上記セッション設立に相当するユーザＩＤ共通化のためのユーザＩＤ共通化要求のデータを作成し、ホームシステム２のユーザＩＤ共通化部１０６Ａとコネクションを張り、ユーザＩＤの共通化作業を行う。

【０１９９】ここで、本実施の形態におけるユーザＩＤ共通化の要求のためのデータの具体例を示す。

１．送信元ネットワークアドレス：遠隔システム４のネットワークアドレス（＝Ｂ）

２．あて先のネットワークアドレス：ホームシステム２のネットワークアドレス（＝Ａ）

３．計算機システムの認証のための署名：遠隔システム４のネットワークアドレスとホームシステム２のネットワークアドレスを遠隔システム４のもつ秘密鍵とホームシステム２の公開鍵を暗号化したもの

４．送信元の計算機システムでのユーザＩＤ：遠隔システム４での自分のユーザＩＤ（＝１０１）

５．あて先の計算機システムでのユーザＩＤ：ホームシステム２での自分のユーザＩＤ（＝１）

６．ユーザＩＤの認証のための署名：遠隔システム４のユーザＩＤとホームシステム２のユーザＩＤを田中さんのもつ秘密鍵で暗号化したもの

【０２００】上記のユーザＩＤ共通化の要求のためのデータのうち、送信元（自システムすなわち遠隔システム４）のネットワークアドレスとユーザＩＤは、自動的に作成される。つまり、自ネットワークアドレスは、ネットワーク部１０３で保持しており、ユーザＩＤは、ユーザ管理部２０３で保持している。

【０２０１】共通化を行う相手（あて先すなわちホームシステム２）のネットワークアドレスとユーザＩＤは、ユーザから情報を得る。

【０２０２】本実施の形態では、計算機システムの認証のための署名は、署名・認証部１０８にて作成する。あて先のシステム（ホームシステム２）のネットワークアドレスと発信元システム（遠隔システム４）のネットワークアドレス（すなわち自システムのネットワークアドレス）はすでに得られているので、これらに加えて、新たにあて先の計算機システム（ホームシステム２）の公開鍵を公開鍵取得部１１０より入手し、自システム（遠隔システム４）の秘密鍵を秘密鍵保存部１０９から得る。ここには、計算機システム秘密鍵保存部２１２から得られた鍵が保管されている。これらから、あて先の計算機システム（ホームシステム２）のネットワークアドレスと発信元計算機システム（遠隔システム４）のネットワークアドレスを発信元の計算機システムの秘密鍵とあて先計算機システム（ホームシステム２）の公開鍵で暗号化してシステム認証のための署名が作成される。

【０２０３】ユーザＩＤの認証のための署名の作成も、署名・認証部１０８にて同様に行う。ユーザの個人秘密鍵は、秘密鍵保存部１０９から得る。ここへは、ユーザが個人秘密鍵入力部２１３に入力することでユーザの個人秘密鍵が得られている。あて先計算機システム（ホームシステム２）上のユーザＩＤと自システム（遠隔システム４）のユーザＩＤは既に得られているので、この２つを個人秘密鍵で暗号化することで署名ができる。

【０２０４】次に、遠隔システム４からユーザＩＤ共通化の要求のためのデータが送られてきたホームシステム２側では、ユーザＩＤ共通化部１０６Ａにて、以下の処理ｄ－１～処理ｄ－４の手順でユーザ共通化の判断と登録を行う。処理ｄ－１　送られてきたデータ利用して、発信元計算機システム（遠隔システム４）のＩＤを認証する。処理ｄ－２　さらに、送られてきたデータを利用して、発信元ユーザの認証をする。処理ｄ－３　上記２つの認証が成功したら、（上記第１の実施の形態におけるアクセス許可条件リストに相当するものがないので）、アクセスが許可されたとし、図１９に示すようにユーザＩＤ対応管理表１０５Ａにアクセス許可データを登録し、送信元である計算機システム（遠隔システム４）にアクセスを許可する旨を通知する。

【０２０５】なお、アクセス許可データとしての登録内容を以下に示す。

１．自計算機システム（ホームシステム２）でのユーザＩＤ

２．対応する外部計算機システム（遠隔システム４）のネットワークアドレス

３．対応する外部計算機システム（遠隔システム４）でのユーザＩＤ

４．有効期間

処理ｄ－４　認証が成功しなければその旨のデータを発信元である計算機システム（遠隔システム４）に返す。

【０２０６】次に上記の処理ｄ－１の認証処理をさらに詳しく説明する。送られてきたデータのうちシステム認証のための署名から、ホームシステム２の秘密鍵と遠隔システム４の公開鍵を用いて署名・認証部１０８にて認証を行う。

【０２０７】ホームシステム２の秘密鍵は、秘密鍵保存

部１０９から得られ、ここには、計算機システム秘密鍵保存部２１２から得られた鍵が保管されている。遠隔システム４の公開鍵は、公開鍵取得部１１０より得る。ここに該当する公開鍵を保存していなければ、ここからネットワーク部１０３を経て外部の公開鍵サーバ（図示せず）より入手する。この２つの鍵を使って上記の署名を復号し、平文を得る。平文が、確かにホームシステム２のネットワークアドレスと遠隔システム４のネットワークアドレスとに一致したときに、認証が成功する。

【０２０８】次に、処理ｄ－２の認証処理をさらに詳しく説明する。処理ｄ－１と同様に、送られてきたデータのうちユーザ認証のための署名を、該当ユーザの公開鍵を使って復号し、平文を得る。この平文が、同時に送られてきたデータ中の送信元のあて先の計算機システムのユーザＩＤと一致するか否かの検査を行い、一致したときに認証が成功する。なお、公開鍵は、公開鍵取得部１１０により得る。

【０２０９】上記の処理ｄ－３は、第２の実施の形態における処理ｂ－４と同様である。ただし、本実施例の形態では第２の実施の形態の個人スケジュール管理を省いているので、有効期間を一律現在時から例えば４時間と設定する。

【０２１０】第２の実施の形態のように、ユーザごとにスケジュール管理表、または、別の指示によって、アクセス許可条件リストを作成し、この表を用いて外部からのホストやユーザなどのアクセス先とアクセス時間を制限してもよい。また、ユーザＩＤの代わりにユーザ名などを用いてもよい。

【０２１１】尚、本実施の形態では、システムの認証にネットワークアドレスまたはシステム名を用いるが、地理的場所（住所）によるアクセス制限も可能である。この場合、別の手段で提供される地理的場所と、これとネットワークアドレスまたはシステム名との対応関係を保持する手段とを組み合わせることで実現できる。これはたとえば、ネットワーク管理システムで保持しているデータベースからの情報提供を受けることで可能となる。このデータベースは、図２３のようにネットワークアドレス、ホスト名、設置場所の関係を管理しており、ネットワークトラブルや、トラフィックス監視などのネットワーク管理業務に利用している。このデータベースを利用すると、「関東地区からの外部アクセス可」とか、「本社会議室のみアクセス可」などの制限が可能になる。この場合、個人スケジュール表にかえて、外部アクセス許可表をユーザごとに作成し、ユーザＩＤ共通化において、認証が成功した後、このアクセス許可表に記載された内容（許可時間と場所）なら外部アクセスを許可する方式となる。

【０２１２】（第４の実施の形態）次に、本発明の第４の実施の形態について説明する。上記第２および第３の実施の形態では、遠隔システム４へ移動したユーザが、ホームシステム２との間でユーザＩＤ共通化を行ったのち、実際の作業をはじめる方式を用いたが、この第４の実施の形態は、ユーザが所望する作業を直接行う方式を用いる。この第３の実施の形態の全体構成は、上述した図１と同様である。

【０２１３】本実施の形態では、計算機システム２，４の内部機能構成は同一であるとし、これを図２４に示す。図２４に示すように、この計算機システム２４０は、入出力部２０１，ローカルログイン２０２，ユーザ管理部２０３，リモートログイン２０４，リモートファイル転送２０６，ファイルシステム２０５，コネクション管理部１０２，ネットワーク部１０３，署名・認証部１０８，公開鍵取得部１１０，計算機システム秘密鍵保存部２１２，秘密鍵保存部１０９，ユーザ・コネクション対応管理部２１１，ユーザＩＤ変換部１０４Ａ，外部アクセス許可判断部１０６Ｂ，外部アクセス検出部１０１，アクセス許可条件リスト１０７から構成される。

【０２１４】上記第１の実施の形態との比較では、通常の処理１００と対応するものは、入出力部２０１，ローカルログイン２０２，ユーザ管理部２０３，リモートログイン２０４，リモートファイル転送２０６，ファイルシステム２０５である。但し、リモートログイン２０４とリモートファイル転送２０６は、ユーザＩＤ変換部１０４Ａから指示されたユーザＩＤの権限で直接起動され、各プログラムの中で再度ユーザＩＤの入力処理をしないように、改造されているものである。図２のネットワークデータ加工・復元部１０４とは、ユーザＩＤ変換部１０４Ａが対応し、秘密鍵保存部１０９に、計算機システム秘密鍵保存部２１２が付加されている。又、図２のセッション情報管理部１０６とは、外部アクセス許可判断部１０６Ｂが相当するが、セッション情報保存部１０５と相当するところはない。又、コネクション管理部１０２には、ユーザ・コネクション対応管理部２１１が付加されている。

【０２１５】両システム２，４をつなぐネットワークプロトコルは、第１～第３の実施の形態と同様、ＴＣＰ／ＩＰとする。従って、ネットワーク部１０３はＩＰ処理を行い、コネクション管理部１０２はＴＣＰの処理を行う。また、ＴＥＬＮＥＴ、ＦＴＰ等のサービスも実行できるものとする。

【０２１６】本実施の形態においても、第３の実施の形態と同様なシステム間の認証機能を有し、所望の処理に先だって、計算機システム間の認証処理を行うが、これは上記第３の実施の形態と同様であるので、ここでの説明は省略する。

【０２１７】いま、ユーザ田中さんが、ホームシステム２上にアカウントを持っているものとする。そのホームシステム２上でのユーザＩＤを１とする。このユーザ田中さんは、遠隔システム４にもアカウントを持っており、その遠隔システム４上のユーザＩＤを１０１とす

る。これら両ユーザＩＤの対応関係は、予め、両システム２，４間で取り決めておき、アクセス許可条件リスト１０７の中に記入しておく。この場合、例えば、ホームシステム２のアクセス許可条件リスト１０７の中には、図１９のようなデータが入っている。

【０２１８】例えば、ユーザ田中さんは、遠隔システム４を利用しており、ホームシステム２のファイルをコピーしたいとき、リモートファイル転送プログラムを利用する。この時の手順は、以下のような処理ｃ－１～処理ｅ－１４となる。なお、この手順にて交換される情報の流れを、図２５に示す。

【０２１９】処理ｅ－１　ユーザ田中さんは、遠隔システム４のリモートファイル転送２０６（クライアント側）をユーザＩＤ＝１０１の権限として起動させる。

【０２２０】処理ｃ－２　そのプログラムは、外部アクセス検出器１０１，コネクション管理部１０２，ネットワーク部１０３，ＬＡＮ１１１を経て相手計算機システム（ホームシステム２）と通信路を設定し（ＩＰデータグラム通信が可能になる），ＴＣＰのコネクション設定を要求する。本実施の形態では、クライアント側の外部アクセス検出器１０１は、素通りで動作しない。

【０２２１】処理ｅ－３　相手計算機システム（ホームシステム２）のネットワーク部１０３を通り、コネクション管理部１０２へ要求がくる。

【０２２２】処理ｅ－４　相手計算機システム（ホームシステム２）のコネクション管理部１０２では、発信元計算機システム（遠隔システム４）とのＴＣＰのコネクションを張り、外部アクセス検出部１０１を通り、リモートファイル転送２０６（サーバ側）を起動しようとする。

【０２２３】処理ｅ－５　ホームシステム２の外部アクセス検出部１０１は、上記のコネクション要求を検出し、接続の可否の判断を外部アクセス許可判断部１０６Ｂに依頼する。外部アクセス許可判断部１０６Ｂでは、コネクション管理部１０２へ、発信元計算機システム（遠隔システム４）のネットワークアドレスとユーザＩＤを要求する。

【０２２４】処理ｅ－６　上記コネクション管理部１０２では、トランスポートレイヤのコネクションを張る段階で発信元計算機システム（遠隔システム４）のネットワークアドレスやコネクション識別子（ポート番号）が得られている。これは、ＴＣＰのプロトコルの仕様に基づくものである。

【０２２５】処理ｅ－７　ホームシステム２の外部アクセス許可判断部１０６Ｂでは、さらに、発信元計算機システム（遠隔システム４）のユーザ・コネクション対応管理部２１１に問い合わせることにより、このコネクションを張った発信元計算機システム（遠隔システム４）のユーザＩＤなどの情報が得られる。このユーザ・コネクション対応管理部２１１の処理は、identificationプロトコル（ＲＦＣ１４１３などで規定）に従って行われているものである。

【０２２６】処理ｅ－８　さらに、ユーザＩＤなどを返答する際に、返答データを署名・認証部１０８にて、自システム（遠隔システム４）の秘密鍵で暗号化して遠隔システム４の署名を付加してから返答する。この返答データの中には送信元システム（遠隔システム４）のネットワークアドレスが平文で含まれている。

【０２２７】処理ｅ－９　受信側計算機システム（ホームシステム２）の外部アクセス検出部１０１は、上記発信元計算機システム（遠隔システム４）のユーザ・コネクション対応管理部２１１からの署名付きデータを署名・認証部１０８にて認証したのち、２つのデータ（発信元ネットワークアドレスとユーザＩＤ）を得る。

【０２２８】処理ｅ－１０　ホームシステム２の署名・認証部１０８では、上記認証は、発信元計算機システム（遠隔システム４）の公開鍵を公開鍵取得部１１０にて取得し、この公開鍵でデータを復号し、その結果が平文で送られてきたネットワークアドレスと一致することで復号が成功し、認証される。成功すると、返答データ中から発信元システムのネットワークアドレスやユーザＩＤなどの情報が平文で得られる。

【０２２９】処理ｅ－１１　得られたデータが前述のアクセス許可条件リスト１０７に登録されているか検索を行う。ここで、更にアクセス条件が付加されていれば（時間など），それも考慮してアクセス可能か否かをチェックする。その可否と、可能な場合の、自システムにおけるユーザＩＤを外部アクセス検出器１０１へ伝える。

【０２３０】処理ｅ－１２　外部アクセス検出部１０１では、検査に合格すると、対応している自システム（ホームシステム２）のユーザＩＤ（この場合ユーザＩＤ＝１）と起動させるプログラム名などをユーザＩＤ変換部１０４Ｂへ伝え、ここで指示された権限で、リモートファイル転送２０６（サーバ側）を動作させ、発信元計算機システム（遠隔システム４）のリモートファイル転送２０６（クライアント側）とコネクションを張り、リモートコピーの処理を開始する。この場合、第２，３の実施の形態と異なり、既に認証が済んでいるので、再度ログイン処理をしないで、認証できた自システム（ホームシステム２）のユーザＩＤ（この場合，ユーザＩＤ＝１）の権限で、アクセス制御を行うことができる。ただし、第２，３の実施の形態のように、再度ログイン処理を行っても構わない。

【０２３１】処理ｅ－１３　外部アクセス許可判断部１０６Ｂで不可の判断が出ると、外部アクセス検出部１０１では、発信元計算機システム（遠隔システム４）に不許可の返事を返し、コネクションの切断をコネクション管理部１０２へ指示する。

【０２３２】処理ｅ－１４　合格した場合、遠隔システ

ム４のユーザは、実際のファイル転送の処理を利用可能になる。

【０２３３】リモートログインプログラムの場合も同様に、外部の計算機システム（遠隔システム４）のネットワークアドレスとユーザＩＤで認証を行ってから、対応する自システムのユーザＩＤを求め、そのユーザＩＤのアクセス権限でリモートログインの処理を行う。

【０２３４】以上説明したように、本実施の形態によれば、管理や計算機システムの構成の異なる複数の計算機システムをネットワークを介して接続した分散環境において、各計算機システムでユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全にファイルなどの個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【０２３５】すなわち、従来、ユーザが外部から計算機システムを利用する場合、計算機システム間のユーザＩＤ管理が独立していると、同一ユーザであっても別々のユーザＩＤを利用しなければならず、不便であった。さらに、互いの計算機システムが広域ネットワークに接続されていると、通信相手を信用することが困難であり、外部からの利用は、再度、ログイン処理を行ってユーザ確認を行うなど、ユーザに手間をかけていた。

【０２３６】本実施の形態では、ユーザＩＤの対応関係を予め、計算機システム間で交換しておき、計算機システム間の認証機能を付加することにより、ユーザの外部からの利用の際には、計算機システム間で認証を行うだけで、同一ユーザのユーザＩＤ対応関係が得られるので、ユーザに認証や、他マシンでのユーザＩＤの入力やパスワードの入力を求めることなく、自動的にユーザＩＤの対応関係の取得とユーザＩＤの変換を行うことが可能になり、互いにユーザ管理が異なるシステムであってもユーザにとっては、再ログイン等の不便さが大幅に軽減されるという効果が得られる。

【０２３７】尚、上記第４の実施の形態では、リモートファイル転送２０６を例にとり説明したが、この実施の形態は直接ユーザがファイル転送を行う場合にも利用できる。例えば、Sun Microsystems社のネットワークファイルシステム（ＮＦＳ）のプロトコルに従ってファイルアクセスを行う場合、マウント処理の時に両計算機システム間で計算機システムの認証を行い、両システム間のユーザＩＤの対応関係を得る。以後、ファイルアクセス命令のパケットごとに、ユーザＩＤ変換部１０４Ｂでユーザ１Ｄを対応したものに入れ替えると、遠隔システム４から利用してもホームシステム２で利用したのと同様なアクセス制御が可能となる。

【０２３８】又、上記第４の実施の形態では、ユーザＩＤの変換処理をホームシステム２（サーバ）側で行ったが、遠隔システム４（クライアント）側で行ってもよい。

【０２３９】また、本発明は上述した各実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【０２４０】

【発明の効果】本発明によれば、管理や構成の異なる複数の計算機をコントロール・ネットワークを介して接続した分散環境において、ユーザが１つの計算機を他の計算機から利用する場合でも、該１つの計算機における資源を、そこでのユーザ識別情報（のアクセス権限）を用いて利用することが可能である。しかも、該１つの計算機でのユーザ識別情報をほとんど意識することなく、他の計算機（のユーザ識別情報）から利用することができる。

【０２４１】また、管理や構成の異なる場合、通常、外部からの不正アクセスを防ぐため、外部のアクセスは厳しく制限されているが、本システムによって、外部からのアクセスは、許可された計算機システムとユーザにだけ可能になり、その管理も容易となる。

【０２４２】したがって、各計算機でユーザ管理やファイル管理が異なるのにも関わらず、ユーザが移動した先の計算機システムにおいて安全に通信ができ、かつ、ファイル等の個人情報を扱えるので、地理的に分散した環境下でも効率よい個人作業支援が可能になる。

【図面の簡単な説明】

【図１】本発明のシステムの全体構成を示す概略ブロック図。

【図２】本発明の第一の実施の形態における図１のシステムの各計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図３】本発明のシステムの別の全体構成を示す概略ブロック図。

【図４】図３のシステムのセキュリティゲートウェイの機能的構成を示すブロック図。

【図５】図３のシステムのセッション情報管理サーバの機能的構成を示すブロック図。

【図６】図３のシステムのホームシステムの機能的構成を示すブロック図。

【図７】図９のシステムのフィルタリングルータの機能的構成を示すブロック図。

【図８】図９のシステムのネットワークデータ処理サーバの機能的構成を示すブロック図。

【図９】図３のシステムの変形構成例を示すブロック図。

【図１０】図１のシステムのクライアント側計算機システムのセッション設立動作における機能的構成を示すブロック図。

【図１１】図１のシステムのサーバ側計算機システムのセッション設立動作における機能的構成を示すブロック図。

【図１２】図１１のサーバ側計算機システムでのセッシ

41

ョン設立動作で使われるアクセス許可条件リストを示す図。

【図１３】図１１のサーバ側計算機システムでのセッション設立動作でセッション情報保存部に保存されるセッション情報を示す図。

【図１４】図１のシステムの計算機システムのセッションを使った通信時における機能的構成を示すブロック図。

【図１５】本発明の第二の実施の形態におけるシステムの各計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図１６】図１５の計算機システムの個人スケジュール管理部で使われるスケジュール管理表を示す図。

【図１７】図１５の計算機システムで使われるアクセス許可条件リストを示す図。

【図１８】図１５の計算機システムで使われるユーザＩＤ共通化要求データを示す図。

【図１９】図１５の計算機システムのユーザＩＤ対応管理表に格納されるアクセス許可データを示す図。

【図２０】本発明の第二の実施の形態における遠隔システムからのリモートファイル転送利用の手順を示すシーケンス図。

【図２１】本発明の第三の実施の形態におけるシステムの各計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図２２】図２１の計算機システムで使われるユーザＩＤ共通化要求データを示す図。

【図２３】図２１の計算機システムで利用可能なネットワーク管理システムのデータベースを示す図。

【図２４】本発明の第四の実施の形態におけるシステムの各計算機システム（ホームシステム、遠隔システム）の機能的構成を示すブロック図。

【図２５】本発明の第四の実施の形態における遠隔システムからのリモートファイル転送利用の手順を示すシーケンス図。

【符号の説明】

２，６０　ホームシステム

42

４　遠隔システム

６　広域ネットワーク

８，１０，１１１　ＬＡＮ

２０，１５０，２１０，２４０　計算機システム

３０　ホームシステムグループ

４０　セキュリティゲートウェイ

５０　セッション情報管理サーバ

７０　フィルタリンググルータ

８０　ネットワークデータ処理サーバ

９０　ルータ

１００　通常の処理

１０１　外部アクセス検出部

１０２　コネクション管理部

１０３　ネットワーク部

１０４　ネットワークデータ加工・復元部

１０４Ａ　ユーザＩＤ変換部

１０５　セッション情報保存部

１０５Ａ　ユーザＩＤ対応管理表

１０６　セッション情報管理部

１０６Ａ　ユーザＩＤ共通化部

１０６Ｂ　外部アクセス許可判断部

１０７　アクセス許可条件リスト

１０８　署名・認証部

１０９　秘密鍵保存部

１１０　公開鍵取得部

１５１　個人スケジュール管理部

１５２　一時的パスワード入力

１５３　一時的パスワード生成

２０１　入出力部

２０２　ローカルログイン

２０３　ユーザ管理部

２０４　リモートログイン

２０５　ファイルシステム

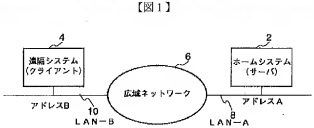
２０６　リモートファイル転送

２１１　ユーザ・コネクション対応管理部

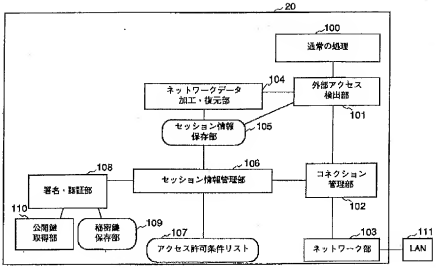
２１２　計算機システム秘密鍵保存部

２１３　個人秘密鍵入力部

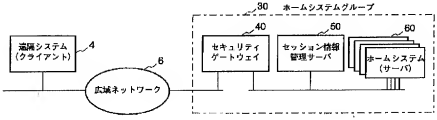
【図１】



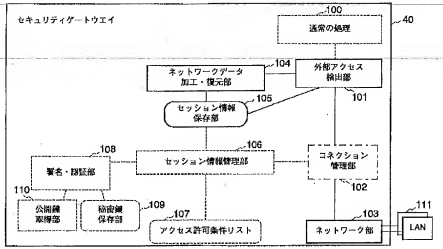
【図２】


20
100
通常の処理
ネットワークデータ
加工・復元部
104
外部アクセス
検出部
101
セッション情報
保存部
105
108
106
署名・認証部
セッション情報管理部
コネクション
管理部
102
110
公開鍵
取得部
秘密鍵
保存部
109
107
アクセス許可条件リスト
103
ネットワーク部
111
LAN

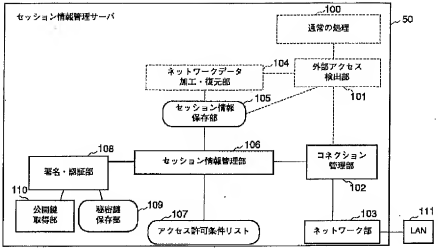
【図３】


30
ホームシステムグループ
端末システム
(クライアント)
4
6
広域ネットワーク
40
セキュリティ
ゲートウェイ
50
セッション情報
管理サーバ
60
ホームシステム
(サーバ)

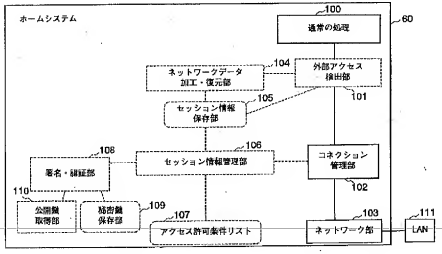
【図４】


セキュリティゲートウエイ
100
40
通常の処理
ネットワークデータ
加工・復元部
104
外部アクセス
検出部
101
セッション情報
保存部
105
108
106
署名・認証部
セッション情報管理部
コネクション
管理部
102
110
公開鍵
取得部
秘密鍵
保存部
109
107
アクセス許可条件リスト
103
ネットワーク部
111
LAN

【図５】



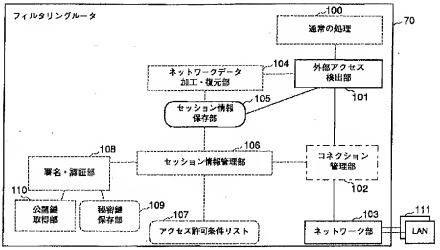
【図６】



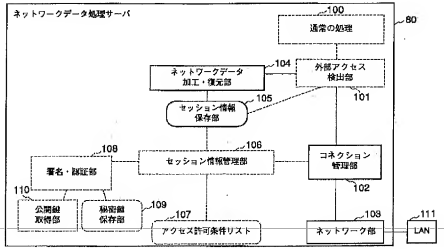
【図１７】

ユーザ ID	外部システムの ネットワークアドレス	一時的パスワード	有効期間
1	B	ABC123	1994.4.1 13:00～17:00
		・ ・ ・	

【図7】



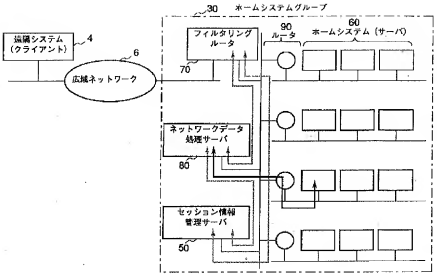
【図8】



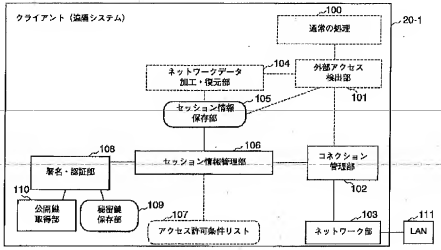
【図19】

自システム上のユーザID	外部システムのネットワークアドレス	外部システムのユーザID	有効期間
1	B	101	1994.4.1 13:00～17:00

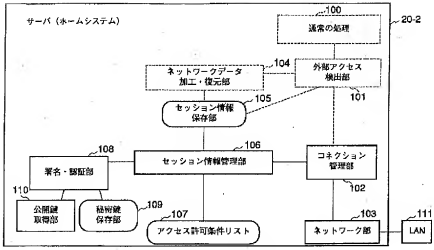
【図９】


30
ホームシステムグループ
協調システム
(クライアント)
4
6
広域ネットワーク
フィルタリング
ルータ
90
ルータ
60
ホームシステム（サーバ）
70
ネットワークデータ
処理サーバ
80
セッション情報
管理サーバ
50

【図１０】


クライアント（協調システム）
100
通常の処理
20-1
ネットワークデータ
加工・復元部
104
外部アクセス
処理部
101
セッション情報
保存部
105
108
署名・認証部
106
セッション情報管理部
コネクション
管理部
102
110
公開鍵
取得部
秘密鍵
保存部
109
107
アクセス許可条件リスト
103
ネットワーク部
111
LAN

【図１１】



【図１２】

ユーザ ID	許可する外部システムのネットワークアドレス	有効期間	その他の条件
1	B	UNTIL 1995.12.31	
2	A～D	1995.1.1～1995.12.31	
3	ALL	ANY TIME	
4	C	1995.9.1 9:00～17:00	TELNET,FTP のみ
5	NONE	NONE	

【図１８】

ユーザID共通化用データである旨の識別子
送信元ネットワークアドレス
あて先ネットワークアドレス
送信元の計算機システムでのユーザID
あて先の計算機システムでのユーザID
一時的パスワード

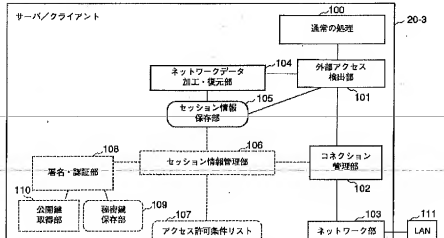
【図２３】

ネットワークアドレス	システム名	設置場所
1000	本社	東京都港区
1001	川崎支店	川崎市川崎区
1002	研究所	川崎市幸区
1003	大阪支店	大阪市北区
⋮	⋮	⋮
2000	会議室 A	本社6階
2001	会議室 B	本社6階
2002	会議室 C	本社7階
⋮	⋮	⋮

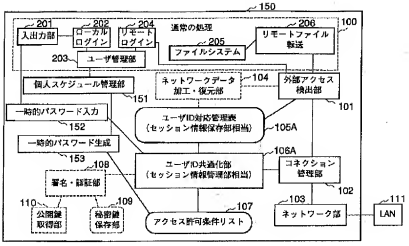
【図１３】

自システムのユーザ ID	許可した外部システムのネットワークアドレス	許可した外部システムのユーザID	セッション鍵	セッション ID	有効期間	その他の条件
1	B	101	ABCDEF	1	UNTIL 1995.12.31	
3	F	43	QWERTY	2	ANY TIME	
4	C	67	ZXCVBN	3	1995.9.1 9:00～17:00	TELNET,FTP のみ
			・	・	・	
			・	・	・	
			・	・	・	
			・	・	・	

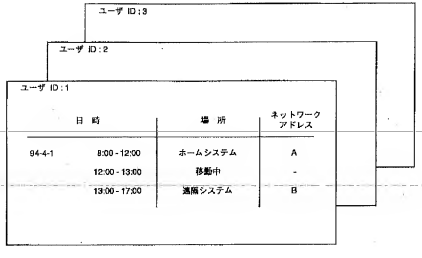
【図１４】



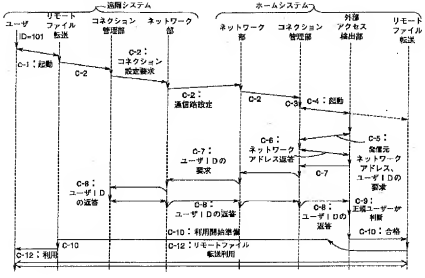
【図１５】


150
100
201
入出力部
202
ローカルログイン
204
リモートログイン
通常の処理
206
リモートファイル転送
205
ファイルシステム
203
ユーザ管理部
個人スケジュール管理部
151
ネットワークデータ加工・復元部
104
外部アクセス検出部
101
一時的パスワード入力
152
ユーザID対応管理表（セッション情報保存部相当）
105A
一時的パスワード生成
153
106A
ユーザID共通化部（セッション情報管理部相当）
コネクション管理部
102
108
署名・認証部
110
公開鍵取得部
109
秘密鍵保存部
107
アクセス許可条件リスト
103
ネットワーク部
111
LAN

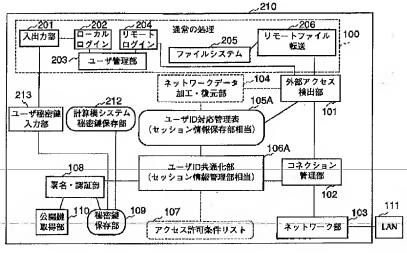
【図１６】


ユーザ ID：3
ユーザ ID：2
ユーザ ID：1
日 時
場 所
ネットワークアドレス
94-4-1
8:00 - 12:00
ホームシステム
A
12:00 - 13:00
移動中
-
13:00 - 17:00
通商システム
B

【図２０】



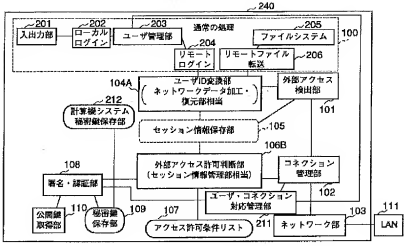
【図２１】



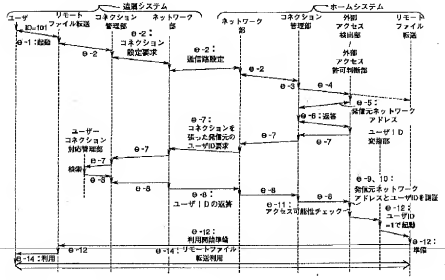
【図２２】

ユーザID共通化用データである旨の識別子
送信元ネットワークアドレス
あて先ネットワークアドレス
計算機システム認証のための署名
送信元の計算機システムでのユーザID
あて先の計算機システムでのユーザID
ユーザID認証のための署名

【図２４】



【図２５】



フロントページの続き

(51) Int. Cl.[6]　　識別記号　　庁内整理番号　　F I　　技術表示箇所
H04L　9/14　　C8-19

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１４年３月１２日（２００２．３．１２）

【公開番号】特開平８－１５３０７２
【公開日】平成８年６月１１日（１９９６．６．１１）
【年通号数】公開特許公報８－１５３１
【出願番号】特願平７－２５５１６９
【国際特許分類第７版】
　G06F　15/00　　330
　
　G09C　 1/00
　H04L　 9/06
　　　　 9/14
【ＦＩ】
　G06F　15/00　　330 B
　　　　　　　　330 C
　G09C　 1/00
　H04L　 9/02　　Z

【手続補正書】
【提出日】平成１３年１０月３０日（２００１．１０．３０）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　通信手段により互いに接続されて互いに通信可能な複数の計算機を有する計算機システムであって、該複数の計算機のうち少なくとも一つの計算機は不正なアクセスから保護されており、該システムが、
他の計算機から該少なくとも一つの計算機へのアクセス要求が許可されるべきかどうかを該他の計算機が前記複数の計算機の内のどれかに基づいて判断し、該少なくとも一つの計算機への通信がそこから該少なくとも一つの計算機へのアクセスが許可された前記複数の計算機中のある計算機からのものかどうか検査するのに用いられるアクセス許可データを生成する管理手段と、
該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機システム。
【請求項２】　前記管理手段は、前記アクセス要求が許可されるべきかどうかを該アクセス要求を行ったユーザにも基づいて判断し、前記通信が前記少なくとも一つの計算機へのアクセスが許可されたあるユーザからのものかどうか検査するのにも用いられる前記アクセス許可データを生成することを特徴とする請求項１記載の計算機システム。
【請求項３】　前記少なくとも一つの計算機にアクセスすることを許可されるべきユーザと計算機の全ての組み合わせを示すアクセス許可条件を格納する格納手段を更に有し、該アクセス許可条件のは前記少なくとも一つの計算機における前記あるユーザのユーザ識別情報を指定し、前記管理手段は該格納手段に格納された該アクセス許可条件に基づいて、該アクセス許可条件を前記アクセス要求が示す前記少なくとも一つの計算機における前記ユーザのユーザ識別情報と比較することにより判断することを特徴とする請求項２記載の計算機システム。
【請求項４】　前記アクセス許可条件は更に前記ある計算機のシステム識別情報を指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機のシステム識別情報と比較することにより判断することを特徴とする請求項３記載の計算機システム。
【請求項５】　前記アクセス許可条件は更に前記ある計算機における前記あるユーザの一時的パスワードを指定し、前記管理手段は前記アクセス許可条件を前記アクセス要求が示す前記他の計算機における前記ユーザの一時的パスワード比較することにより判断することを特徴とする請求項３記載の計算機システム。
【請求項６】　前記アクセス許可条件は更に前記他の計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記少なくとも一つの計算機におけるユーザのユーザ識別情報及び該有効期間を含んだ前記アクセス許可データを生成することを特徴とする請求項３記載の計算機システム。

【請求項７】　前記アクセス要求は、発信元システム識別情報、発信先システム識別情報、及びシステム識別署名データを示し、前記管理手段は該システム識別署名データを認証することにより判断することを特徴とする請求項１記載の計算機システム。

【請求項８】　前記少なくとも一つの計算機におけるあるユーザのユーザ識別情報を示すアクセス許可条件を格納する格納手段を更に有し、前記アクセス要求は、発信先ユーザ識別情報及びユーザ識別署名データを示し、前記管理手段は該ユーザ識別署名データを認証し、該発信先ユーザ識別情報を該格納手段に格納された該アクセス許可が示す該ユーザ識別情報と比較することにより判断することを特徴とする請求項２記載の計算機システム。

【請求項９】　前記アクセス要求は更に、発信元ユーザ識別情報も示し、前記ユーザ識別署名データは、前記発信元ユーザ識別情報と前記発信先ユーザ識別情報を前記ユーザの秘密鍵を使って暗号化して求められたものであり、前記管理手段は該ユーザ識別署名データを前記ユーザの公開鍵を使って復号化することにより認証することを特徴とする請求項８記載の計算機システム。

【請求項１０】　前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機のシステム識別情報及び前記他の計算機における前記ユーザのユーザ識別情報を含んだ前記アクセス許可データを生成することを特徴とする請求項９記載の計算機システム。

【請求項１１】　前記アクセス許可条件は更に前記他の計算機における前記あるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を更に含んだ前記アクセス許可データを生成することを特徴とする請求項１０記載の計算機システム。

【請求項１２】　前記管理手段が前記アクセス要求を許可されるべきと判断したとき、該管理手段は前記他の計算機から前記ユーザによる前記各計算機への通信に使われる鍵データを含んだ前記アクセス許可データを生成することを特徴とする請求項１記載の計算機システム。

【請求項１３】　該少なくとも一つの計算機への通信が該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して前記他の計算機から間接的になされたものかを検出し、該通信が間接的になされたものである場合、該通信が正当なアクセスであるかどうかを前記メモリ手段に記憶した前記アクセス許可データに基づいて検査して正当なアクセスを許可する検出手段と、
を有することを特徴とする請求項１記載の計算機システム。

【請求項１４】　前記メモリ手段は、前記ある計算機における前記あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報との組を記憶し、
前記検出手段は、前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を前記メモリ手段が記憶しているとき、前記アクセスを正当と判定することを特徴とする請求項１３記載の計算機システム。

【請求項１５】　前記メモリ手段は更に、前記ある計算機における前記あるユーザのための前記アクセス許可データと対応する鍵データを記憶し、
前記少なくとも一つの計算機は更に、前記検出手段が該アクセス許可データに基づいて前記アクセスを正当と判定したとき、前記アクセスの通信データを前記鍵データを使って加工するデータ加工手段を有することを特徴とする請求項１３記載の計算機システム。

【請求項１６】　前記メモリ手段は更に、前記他の計算機におけるあるユーザから前記少なくとも一つの計算機への通信の有効期間を指定し、前記管理手段は該有効期間を記憶し、
前記検出手段は、該メモリ手段に記憶した該有効期間に基づいて、前記アクセスを正当と判定することを特徴とする請求項１３記載の計算機システム。

【請求項１７】　複数の計算機群がネットワークにより互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機群のうち少なくとも一つの計算機群が、
他の計算機群の計算機から該少なくとも一つの計算機群の計算機へのアクセス要求が許可されるべきかどうかを該他の計算機群が前記複数の計算機群の内のどれかに基づいて判断し、該少なくとも一つの計算機群の計算機への通信がそこから該少なくとも一つの計算機群の計算機へのアクセスが許可された前記複数の計算機群の内の一計算機群の計算機からのものかどうか検査するのに用いられるアクセス許可データを生成するデータ管理サーバと、
前記データ管理サーバにより生成された該アクセス許可データに対応して鍵データを記憶するメモリ手段と、該少なくとも一つの計算機群の計算機への通信が正当なアクセスであるかどうかを前記アクセス許可データに基づいて検査して正当なアクセスを許可するとともに、正当なアクセスの通信データを前記鍵データを使って加工する手段と、を含むセキュリティゲートウェイと、
をなすことを特徴とする計算機システム。

【請求項１８】　複数の計算機がネットワークにより互いに接続されて互いに通信可能に構成された計算機システムにおける計算機であって、
他の計算機から該計算機へのアクセス要求が許可されるべきかどうかを該他の計算機が前記複数の計算機の内のどれかに基づいて判断し、該計算機への通信がそこから該計算機へのアクセスが許可された前記複数の計算機中の一つからのものかどうか検査するのに用いられるアクセス許可データを生成する管理手段と、

該管理手段により生成されたアクセス許可データを記憶するメモリ手段と、を有することを特徴とする計算機。

【請求項１９】　複数の計算機が通信手段により互いに接続されて互いに通信可能に構成された計算機システムであって、該複数の計算機のうち少なくとも一つの計算機が、

該少なくとも一つの計算機へのアクセスが該少なくとも一つの計算機において直接的になされたものか、前記通信手段を介して他の計算機から間接的になされたものかを検出し、間接的になされたものである場合、該アクセスが正当であるかどうかを判定し、正当と判定された場合、該アクセスを許可する検出手段と、

そこからあるユーザによる該少なくとも一つの計算機へのアクセスが許可されたある計算機における該あるユーザの外部ユーザ識別情報と、該ある計算機の外部システム識別情報と、該あるユーザの該少なくとも一つの計算機における内部ユーザ識別情報との組を記憶するメモリ手段であって、前記検出手段は前記アクセスの通信データが示すユーザ識別情報とシステム識別情報に一致する外部ユーザ識別情報と外部システム識別情報の組を該メモリ手段が記憶しているとき前記アクセスを正当と判定するものと、

前記検出手段が前記アクセスを正当と判定したとき、前記アクセスの通信データが示すユーザ識別情報を該ユーザ識別情報と一致する前記外部ユーザ識別情報に対応する前記内部ユーザ識別情報に変換する変換手段と、

を有することを特徴とする計算機システム。